Selection of a new hardware and software platform for railway interlocking

Arghya Kamal Bhattacharya

School of Electrical Engineering

Thesis submitted for examination for the degree of Master of Science in Technology.

Espoo 27.04.2020

Supervisor

Prof. Valeriy Vyatkin

Advisor

MSc. Tommi Kokkonen

Aalto University
School of Electrical Engineering

Aalto University, P.O. BOX 11000, 00076 AALTO
www.aalto.fi
Abstract of the master's thesis

Author Arghya Kamal Bhattacharya

Title Selection of a new hardware and software platform for railway interlocking

Degree programme Automation and Electrical Engineering

Major Control, Robotics and Autonomous Systems **Code of major** ELEC3025

Supervisor Prof. Valeriy Vyatkin

Advisor MSc. Tommi Kokkonen

Date 27.04.2020 **Number of pages** 82+34 **Language** English

Abstract

The interlocking system is one of the main actors for safe railway transportation. In most cases, the whole system is supplied by a single vendor. The recent regulations from the European Union direct for an "open" architecture to invite new game changers and reduce life-cycle costs.

The objective of the thesis is to propose an alternative platform that could replace a legacy interlocking system. In the thesis, various commercial off-the-shelf hardware and software products are studied which could be assembled to compose an alternative interlocking platform. The platform must be open enough to adapt to any changes in the constituent elements and abide by the proposed baselines of new standardization initiatives, such as ERTMS, EULYNX, and RCA. In this thesis, a comparative study is performed between these products based on hardware capacity, architecture, communication protocols, programming tools, security, railway certifications, life-cycle issues, etc.

Keywords railway, interlocking, PLC, OS, IDE, ERTMS, EULYNX, RCA

Preface

I would like to thank my supervisor Prof. Valeriy Vyatkin for guiding the thesis with his valuable and insightful suggestions.

This thesis was conducted at Mipro Oy. I would like to thank my thesis advisor Tommi Kokkonen and my manager Sami Hyyryläinen at Mipro Oy for suggesting the topic. The thesis was made possible with their persistent reviewing and encouragement. I would also like to acknowledge all my colleagues for their intuitive technical inputs.

Finally, I would like to thank my friends and family for cheering me up throughout this journey.

Mikkeli, 27.04.2020

Arghya Kamal Bhattacharya

Contents

Abbreviations

API	Application Programming Interface
APS	Advanced Protection System
ATO	Automatic Train Operation
ATP	Automatic Train Protection
BSP	Board Support Package
CBTC	Communications-Based Train Control
CCS	Command and Control Systems
CENELEC	European Committee for Electrotechnical Standardization
CI	Counter Input
COTS	Commercial Off-The-Shelf
CP	Control Processor
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CSP	ControlSafe Platform
DI	Digital Input
DO	Digital Output
E/E/PE	Electrical/Electronic/Programmable Electronic
ERTMS	European Rail Traffic Management System
ETCS	European Train Control System
EU	European Union
EUC	Equipment Under Control
EUG	ERTMS User Group
EVC	European Vital Computer
FSoE	FailSafe over EtherCAT
FTIA	Finnish Transport Infrastructure Agency
GSM-R	Global System for Mobile Communications – Railway
IDE	Integrated Development Environment
IEC	International Electrotechnical Committee
IM	Infrastructure Manager
I/O	Inputs/Outputs
IOP	I/O Processor
OS	Operating System
PACY	Process Data Application Framework
PLC	Programmable Logic Controller
QOS	QNX OS for Safety
RAMS	Reliability, Availability, Maintainability, and Safety
RBC	Radio Block Centre
RCA	Reference CCS Architecture
RTOS	Real-Time Operating System
SCADE	Safety Critical Application Development Environment
SIL	Safety Integrity Level
TCS	Traffic/Train Control System

1 Introduction

For the past six decades, rail transportation in terms of passenger and freight services are in decline compared to the alternative options via road and air. In recent years, the European Union (EU) has put more impetus on rail transport, due to rising fuel prices and environmental concerns, by opening up the market to new players. In the words of Antonio Tajani, the former president of the European Parliament, the EU "will therefore spare no effort in building the rail network of the future in cooperation with all rail sector partners" [1]. This necessitated the European Union Agency for Railways (ERA) to address policies like the Trans-European Transport Network (TEN-T) to use railways, amongst other transportation modes, as a tool for a coherent socio-economic integration of the continent. TEN-T stipulates to build the "Core Network" corridor by 2030 and targets for a shift of 30% to rail freight from roadways for journeys over 300km [2]. In Finland, this network includes Saimaa waterway area, Helsinki and Turku airports, Kouvola combined road and rail transport terminal, ports of Hamina-Kotka, Helsinki, Turku, and Naantali [3].

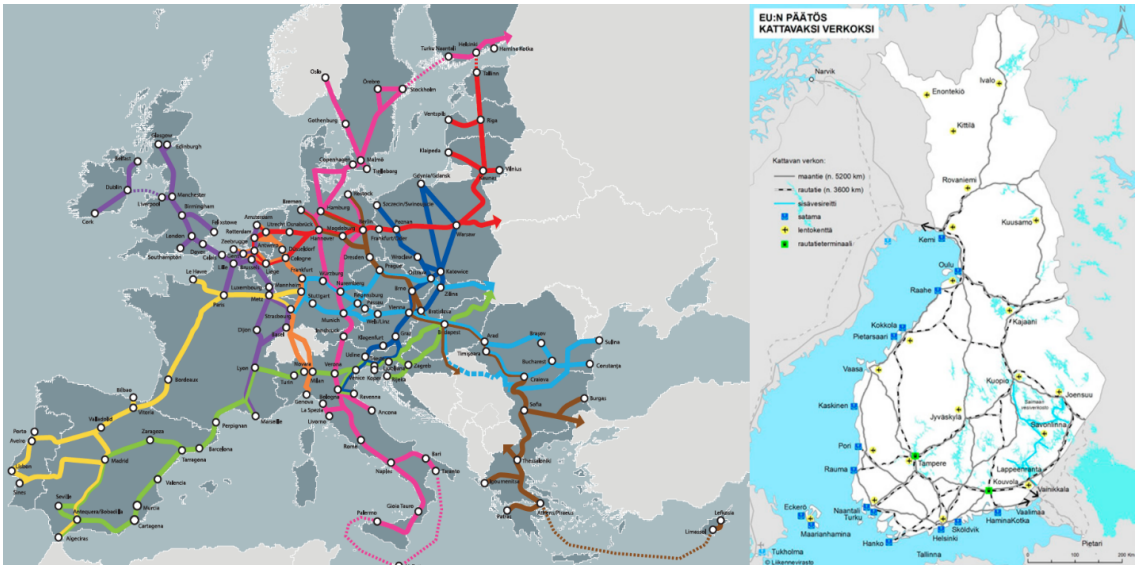

Figure 1: The core network corridors in the EU and Finland [4], [5].

The Automatic Train Protection (ATP) system is the backbone of railway transportation which ensures correct and safe operation across the network. Traditionally, a particular ATP is supplied by a single manufacturer for a specific country or region. As a result, long-running inter-regional trains have become equipped with numerous ATPs, incurring huge costs. On the other hand, there are constant efforts to integrate new technologies into the respective ATPs to facilitate Pan-European rail carriage. European Rail Traffic Management System (ERTMS), one of the horizontal properties of TEN-T, aims to substitute different national ATPs with a common interoperable system. Also, there are attempts to modularize national interlocking systems with standardized interfaces by a consortium of European infrastructure managers, EULYNX.

1.1 Thesis Scope and Objective

Mipro Oy is specialized in providing signalling and interlocking solutions for metro and railway applications. These are certified with the highest levels of safety. Mipro's TCS-O is developed on a safety programmable logic controller (PLC) package supplied by HIMA Paul Hildebrandt GmbH. It contains hardware (HIMax and HIMatrix) and software (proprietary operating system and SILworX suite with IEC 61131-3 language support) components. As of now, the TCS-O is delivering satisfactory performances. But, since the setup is vendor-locked, Mipro commissioned this thesis to find out a suitable alternative platform with enhanced capacity, modularity, and flexibility. The present system possesses some bottlenecks, such as developing applications with high-level programming, integrating with interfaces of other any other interlocking systems which is of paramount importance in the wake of ERTMS, EULYNX, and RCA initiatives, availing different application programming interfaces (API) via operating systems, etc.

The objective of the thesis is to discover commercial off-the-shelf (COTS) hardware and software (operating system and development environment) components that could be assembled to constitute an alternative interlocking platform. These products should preferably be pre-certified as per the railway safety standards to reduce the efforts from the procurer's side in terms of time and money. The constituents of the platform must be "open" enough to adapt to any changes, e.g. the hardware must be compatible with most of the commercially available operating systems, to enable the system integrator with flexibility to change as per the project requirements. The alternative system should also comply with the proposed baselines of ERTMS, EULYNX and RCA. In this thesis, a comparative study is performed between these products based on hardware capacity, architecture, communication protocols, programming tools, security, railway certifications, price, and life-cycle issues.

1.2 Research Questions

Following research questions are raised in the thesis:

1. Why the current platform might not be sufficient in the future?
2. What are the possible alternatives available to replace the current platform?
3. How the possible solutions are chosen?

The first research question is addressed in Chapter 1.1. The answer for the second question is spanned across Chapters 5, 6, and 7. The final question is responded via Chapters 4 and 8.

1.3 Thesis Contribution

The contribution of the thesis is about selecting and reviewing different COTS and safety-certified hardware and software elements that can be used for railway interlocking applications. To this extent, the author of the thesis has chosen 2 hardware platforms, 4 real-time operating systems and 4 integrated development environments to be examined. The author of the thesis has devised a mechanism to compare the combinations of these products based on benchmarks, such as PLC architecture, I/O capacity, communication protocols, software architecture and framework, programming languages, development tools, certifications, applications, brand value, life-cycle issues, etc. From the comparative analysis, best and worst possible combinations are discussed. The author of the thesis has mentioned about the factors which were not accounted while comparing.

1.4 Thesis Structure

The next chapter in the thesis is the background which provides a basic idea about railway interlocking, safety standards in railway, and newly approved specifications for interlocking architectures. The third chapter depicts the hardware, software, and communication protocols used in the present system. The fourth chapter illustrates the methodology used in this thesis for comparing different metrics of the proposed alternative system. The fifth, sixth and seventh chapters are dedicated in describing different alternative hardware, operating systems, and development environment platforms reviewed in the thesis. The eighth chapter covers the comparative analyses between the above-mentioned products and the selection of the possible composite alternative platform/s. The final chapter draws a conclusion on the study, mentioning future tasks that could be carried out.

2 Background

Interlocking is defined as a manual or automatic arrangement "of signals and signal appliances so interconnected that their movements must succeed each other in proper sequence and for which interlocking rules are in effect" [6]. A signalling system is formed by "one or more interlockings or signalling apparatuses (even if they do not form an interlocking system), which protects traffic movements" [7]. In other words, an interlocking system acts as the control system for ensuring a safe rail traffic movement by sending commands to signals and other devices situated on the sides of a railway track. Following the lines of technological evolution, railway interlocking has gone through several generational changes in the past 160 years. From the early days of manual levers and electropneumatic setups to control signals and other devices, interlocking has progressed into an "all-electric" relay-logic based system and later on has embraced the advantages offered by electronic controllers. In this section, the basic norms of an interlocking system are described, followed by the standards required to develop it.

2.1 Railway Signalling and Interlocking Principles

The Finnish Transport Infrastructure Agency (FTIA/Väylä) states that an interlocking system [8] must

1. be able to control and monitor signalling elements,
2. ensure safety via interdependencies between signalling elements,
3. ensure one failure does not concur uncontrolled hazardous situation, and
4. fulfill all the requirements for safety integrity level (SIL).

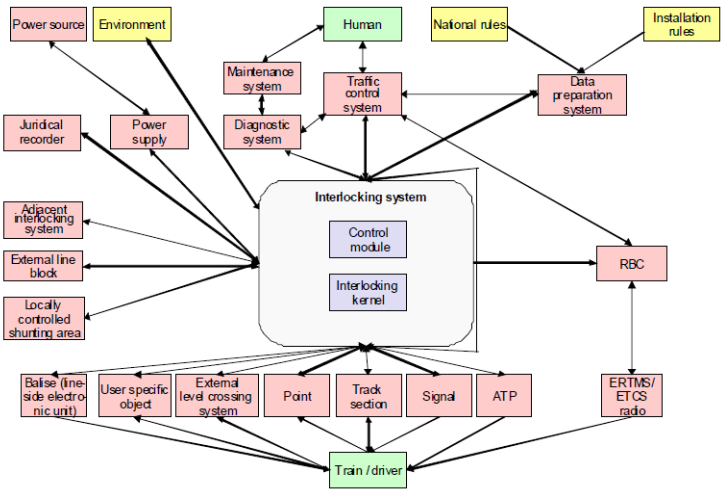

Figure 2: The interlocking system context diagram [9].

The FTIA prescribes the Interlocking System Context Diagram, illustrated in Figure 2, as a qualitative requirement [9]. In the diagram, a typical interlocking system is accompanied by the Traffic Control System (TCS) and physical elements. The functional objects, physical and non-abstract objects, abstract objects, and secondary areas, such as trains and human factors are represented by blue, pink, yellow, and green coloured boxes, respectively. It can exchange train information with adjacent interlocking systems. The interlocking system consists of an interlocking kernel and control module. The interlocking kernel, includes safe and non-safe functions to perform detection and steering, locking functions, and contains information concerning permission to move the train from one track section to another (movement authority). The control module is formed with non-safe functions and provides isolation between the interlocking kernel and the TCS, giving the flexibility to use products from different manufacturers. The TCS receives commands from signallers, remote control systems, and automatic route-setting systems and relays it to the interlocking system, which in turn sends the statuses back. There are some dedicated systems attached with the TCS, such as the diagnostic system which is used for logging faults in interlocking systems and physical elements and sending the information to external elements such as maintenance systems for treating states and faults; the data preparation system which is an offline method to generate data for configuring a specific interlocking system as per the national and installation rules; the block system which controls train movements between interlocking areas and open line, etc. The context diagram also contains physical objects which are described briefly in the following texts.

Signal: It is the visual status of the movement authority, directing the driver to proceed as per the requirements. There are different types of signals, such as main, shunting, and others.

Track Section: For a railway network, the tracks are divided into sections. The train can enter a particular track section if and only if it is “vacant”. Track vacancy is informed to the interlocking system by track circuits and axle counters. The former detects the presence of a train when a relay, placed in between the rails which are electrified, is de-energized. Axle counter is generally installed at the beginning and end of a track section. It detects train presence by counting every axle of the train.

Balise: It is a passive device which is typically placed in between the rails for storing data regarding geographical location, track geometry, and corresponding speed limits. There is an interface between the interlocking system and balise, known as the Lineside Electronic Unit (LEU). The LEU sends information both ways via digital telegrams. Eurobalise is a special variant of balises which conforms to the requirements of the European Rail Traffic Management System. It exchanges information with on-board systems via a Balise Transmission Module (BTM) situated under the body of a train. Depending on the type of data being transmitted, there are different types of balises. In Finland, Bombardier’s EBICAB 900 type balises are used [10].

Automatic Train Protection (ATP): This system monitors whether the train speed is complying with the permitted value and applies braking conditions in case of over-speeding . Balises form the integral part of an ATP. In Finland, the ATP is known as ATP-VR/RHK – Junankulunvalvonta (JKV) which permits maximum speeds of 220 km/h and 120 km/h for passenger and freight trains, respectively [11].

Point: This electromechanical system routes a train from one track to another, as per the request sent by the interlocking system.

Radio Block Centre (RBC): It is used at the ERTMS level 2 installations and acts as an intermediary between the interlocking system and the on-board train system. It is presented in in Chapter 2.3.1.

ERTMS/ETCS radio: It is the communication channel of RBC to exchange data with the on-board train system. It is explained in Chapter 2.3.1.

Juridical Recorder: This system timestamps and chronologically records all the incoming data from the interlocking system, TCS, RBC, trackside elements, and adjacent interlocking systems. The recorded data, such as detected and steering values of the trackside elements, power supply voltages, failures, etc. is used for root causes analysis in case of catastrophes [12].

User Specific Object: It includes elements, such as automatic warning system, hotbox detectors, monitors for point-handle housings, etc.

Apart from the above-mentioned elements, the context diagram includes critical objects, such as level crossing systems and required power supplies. The diagram also takes into consideration the country-specific operating and signalling rules, installation rules, and environmental factors in terms of temperature, vibration, and electromagnetic interference. The design of a railway network must be devised in such a way that the required figures for reliability, availability, maintainability, and safety (RAMS) are achieved as per the standards discussed in the next section.

2.2 Safety Standards in Railways

A safety-critical system is a special system where a failure can incur injury, loss of life or serious environmental damages [13]. Until the mid-1980s, no safety-critical system was controlled by a software-based Programmable Electronic System (PES). International Electrotechnical Committee's Advisory Committee of Safety (IEC ACOS) installed a conglomeration of subcommittees, such as Working Group 9, Working Group 10, and IEC SC65A to focus on how to implement safety notions in software and leverage its obvious advantages in a safety-critical system. As a result, IEC 61508 was conceived in 1998 with a generic approach for all safety life-cycle activities in a safety-critical system. Before that standard, there were different nation-specific approaches to system safety. IEC 61508 presented a standardized framework for equipment suppliers and system designers to follow a scientific approach

in identifying and quantifying the risks associated in a system. It is the foundation for the other industry-specific standards. The railway safety standards are prepared by the European Committee for Electrotechnical Standardization (CENELEC) in the forms of EN 50126, EN 50128, and EN 50129. There is also a dedicated standard, EN 50159, for the communication of safe-critical information. In the following texts, these standards will be discussed.

2.2.1 IEC 61508: 2010

The title of the standard reads as "Functional safety of electrical/electronic/programmable electronic safety-related systems" [14]. The standard defines all the equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities as equipment under control (EUC). It is associated with a control system which takes inputs from the process and generates outputs for the EUC to act as planned. There are risks associated with an EUC. A risk is a probabilistic measure of the occurrence and severity of harm/s, which is/are caused by hazard/s leading to direct or indirect potential damages to human beings or the environment. Risks could be tolerable or unacceptable depending on societal values. Safety is defined as freedom from unacceptable risks. IEC 61508 is focused on functional safety, which is one of the three types of system safety [15]. For functional safety, preventive measures known as safety functions are implemented by electrical/electronic/programmable electronic (E/E/PE) safety-related systems to reduce the risks and establish a safe state for the EUC. There could be some risks remaining after these measures, known as residual risks. Functional safety looks into the E/E/PE system safety throughout its life-cycle in a systematic manner as shown in Figure 3.

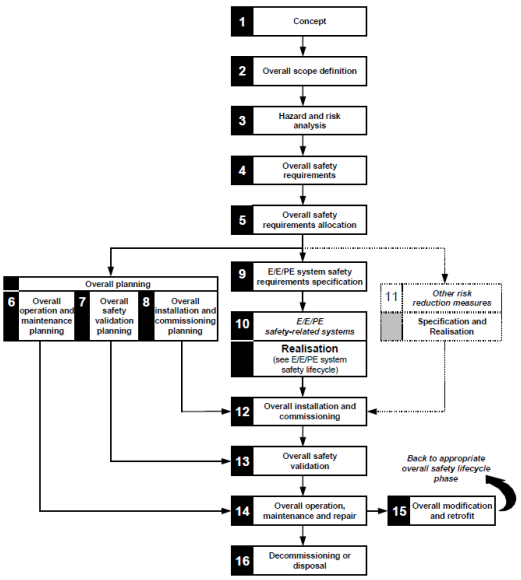

Figure 3: Overall safety life-cycle [14].

Failures in a functional unit prevent the safety functions to be implemented. There are different types of failures depending on the nature, origin and consequences of them, such as random hardware failure, systematic failure, dangerous failure, safe failure, dependent failure, soft errors, etc. IEC 61508 proposes various failure analysis techniques, e.g. Failure Modes and Effects Analysis (FMEA), Event Tree Analysis (ETA), Failure Modes, Effects and Criticality Analysis (FMECA), Fault Tree Analysis (FTA), Reliability Block Diagram (RBD), etc. Depending on the demand for the safety function to establish a specific safe state in the EUC, there are different modes of operation. If the frequency of demands is less than once every year then the specific mode is called as the low demand mode, otherwise, it is a high demand mode. The probability of an E/E/PE safety-related system to perform the required safety functions is quantified by four discreet SIL levels as shown in Table 1. Unlike the MISRA guidelines, in IEC 61508 the SIL is allocated not on the basis of the effects of the failures, but the amount of risk reduction it is targeting to achieve. For low demand mode of operation, the SIL is calculated on the basis of the probability of dangerous failure on demand, whereas probability of a dangerous failure per hour is used for high demand mode.

Table 1: Safety integrity levels.

SIL	Low demand mode of operation	High demand mode of operation
	Probability of failure to perform its design function on demand	Probability of a dangerous failure per hour
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

The voting mechanism is a means to add redundant channels in the system to facilitate fault tolerance. In a MooN voting system, at least M out of N channels should agree about an action before a control system can execute it. 2oo2 and 2oo3 are the most popular voting architectures for any safety-critical system. If a diagnostic system is attached with the architecture then the letter "D" is added in the naming, e.g. 2oo2D. IEC 61508 exemplifies calculations of the average frequency and probability of dangerous failures in low and high demand modes of operations for 1oo1, 1oo2, 2oo2, 1oo2D, 2oo3 and 1oo3 architectures to assign respective SIL. The annexes of the standard are listed in Appendix C.1.

The standard is divided into seven parts as following,

Part 1: "General requirements"

Part 2: "Requirements for electrical/electronic/programmable electronic safety-related systems"

Part 3: "Software requirements"

Part 4: “Definitions and abbreviations”

Part 5: “Examples of methods for the determination of safety integrity levels”

Part 6: “Guidelines on the application of IEC 61508-2 and IEC 61508-3”

Part 7: “Overview of techniques and measures”

2.2.2 EN 50126: 2017

The title of this two-part standard reads as “Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)” [16]. The first part describes the “Generic RAMS Process” and the second part is about the “Systems Approach to Safety”. The RAMS specifications define rail capacity under certain circumstances, determine the maintenance costs, and establish reliable systems. RAMS can be thought of a set of “confidence indices” of a system. This standard specifies targets in terms of RAMS parameters and illustrates methods to achieve them. The RAMS parameters are as follows:

Reliability: It is defined in terms of Mean Time Between Failures (MTBF) which is the expected time between two failures for a repairable system.

$$MTBF = \frac{\sum (start\ of\ downtime - start\ of\ uptime)}{number\ of\ failures}$$

Availability: It is expressed in terms of MTBF and Mean Down Time (MDT), which is the average time during which the system was not operational.

$$A = \frac{MTBF}{MTBF + MDT}$$

Maintainability: It is defined in terms of Mean Time To Repair (MTTR) which is the average time required to repair a component under maintenance.

Safety: It is expressed in terms of the SIL which has been mentioned in IEC 61508.

Figure 4 describes different factors influencing RAMS in the different phases of a railway system life-cycle. This standard illustrates methods, e.g. cause/effect diagrams to define these factors and calculate the effect on the RAMS parameters. Like IEC 61508, EN 50126 illustrates a system life-cycle where the system goes through different phases from the initial concept and system definitions, to decommissioning and disposal. The standard also specifies responsible authorities for each phase, e.g. the risk analysis is carried out by the customer and contractor, whereas the manufacturing and installation duties lie with the suppliers, main- and sub-contractors. The life-cycle is also represented as a V-model. EN 50126 estimates the investment, operating and maintenance costs of a railway system over its complete life-cycle. The annexes of the standard are listed in Appendix C.2.

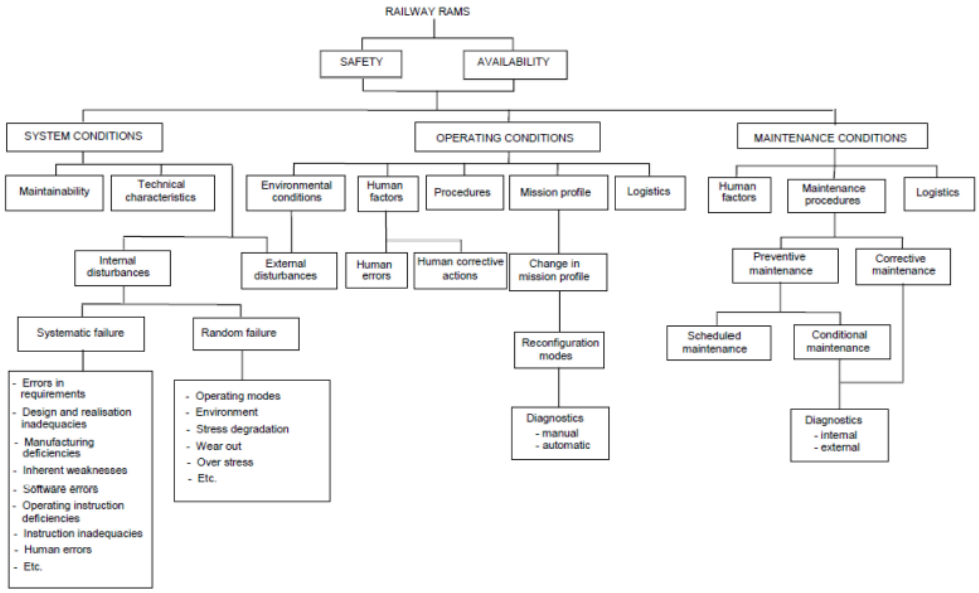

Figure 4: Factors influencing railway RAMS [16].

2.2.3 EN 50128: 2011

The title of the standard reads as "Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems" [17]. It enlists the requirements for a safety-related software to be developed, deployed and maintained throughout the system life-cycle. The term "software" encompasses operating systems, high, low and special purpose application programming, firmware, and supporting tools. Depending on the measures and techniques used in the software, EN 50128 ratifies it between safety integrity levels 0 to 4. The system where the software will be developed shall be defined as per, functions and interfaces; application conditions, configuration or architecture of the system; hazards to be controlled; safety integrity requirements; apportionment of requirements and allocation of SIL to software and hardware; timing constraints, etc. EN 50128 recommends some functional steps as shown in Figure 5 for developing applications of high integrity.

Initially, the software requirements are specified and then a safety policy is drawn up in the software architecture. After allocating safety functions to different parts, the software is designed, developed and tested as per the software quality assurance plan, safety integrity level, and life-cycle. Then the software functionalities are verified and deployed on to the target hardware platform. EN 50128 elaborates important activities for the software development, such as testing, verification, validation, assessment, quality assurance, modification, and change control.

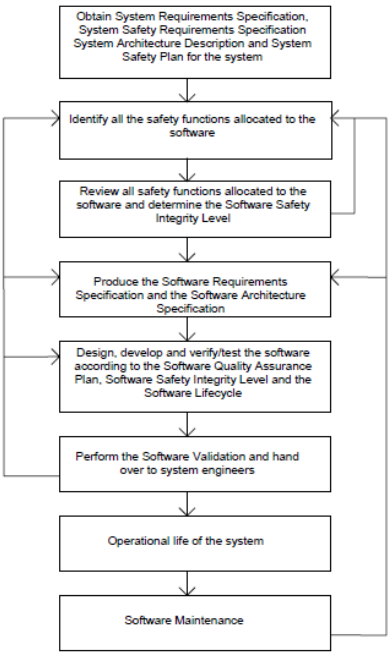

Figure 5: Software route map [17].

EN 50128 classifies software tools into the following classes:

Tool Class T1: It does not affect the executable code and data of the safety-related software, e.g. a text editor or a design support tool which is not equipped with code generation capabilities.

Tool Class T2: It is used for testing and verification purposes of the executable code. A faulty T2 does not generate any errors for the under-testing code. The examples are static analyzers, code coverage tools, etc.

Tool Class T3: This tool directly or indirectly affects the executable code, e.g. a source code compiler which integrates a run time package into the code. This is an important parameter to choose an operating system or development environment for an alternative platform. The safety certificates must have a clear mention of the testing of T3 tools.

The Annex A of EN 50128 guides about a range of techniques or tools to be used for a particular application with a required SIL. It specifies that for developing a safe software application, high-level programming languages, e.g. ADA, MODULA, PASCAL, and graphical languages, e.g. Sequential Function Chart and State Charts are “highly recommended”. C, C++, C# , JAVA, and diagrammatic languages e.g. Ladder Diagram, Functional Block Diagram and Statement List are “recommended”. EN 50128 does not recommend to use PL/M and BASIC as a programming language. The annexes of the standard are mentioned in Appendix C.3. The lists of software design techniques and programming languages are listed in Tables C9 and C10, respectively.

2.2.4 EN 50129: 2018

The title of the standard reads as “Railway applications—Communication, signalling and processing systems—Safety related electronic systems for signalling” [18]. This document enlists the conditions for different electronic components present in a railway system to be accepted and approved as per required safety standards. The standard is based as per the system life-cycle described in Part 1 of IEC 61508, and follows various sections of EN 50126. EN 50129 introduces the concept of the safety case. It is a set of evidences used for justifying the safety of a system under certain circumstances. The safety case is an important deliverable from the rail system manufacturers or IMs. It is approved by an Independent Safety Assessor (ISA) and authorized by national or regional transportation authorities. There are different types of safety cases as presented in the Table 2.

EN 50129 standard prescribes the requirements for a systematic quality management approach to minimize the possibility of systematic faults, and to keep the system life cycle under control by focusing into organizational structure, inspection and testing, documentation, records, etc. The safety management of the system is based on the traditional V-model and controlled by an independent authority with competent personnel to check for safety compliance from all parts of the system regarding safety plan, hazard log, safety requirements specification, safety verification and validation, safety justification, operation, and maintenance. The standard illustrates presentation of a safety evidence report, which showcases correct functional operations with specified safety requirements against random hardware faults or external influences. It also includes a list of constraints for the safety case and safety qualification tests. Before a system is sent for safety acceptance and approval procedures, a document called as Safety Assessment Report (SAR) will be prepared based on all the evidence for quality management, safety management, and functional and technical safety. EN 50129 also includes the measures to deal with unauthorized accesses resulting from physical and IT-Security communications. The annexes of the standard are listed in Appendix C.4.

Table 2: Different safety cases [19].

Safety Case	Prepared By	Approved By	Authorized By
Generic Product Safety Case	Manufacturer	ISA	Notified Body (NoBo) (Europe)
Generic Application Safety Case	Manufacturer	ISA	Not relevant
Specific Application Safety Case	Manufacturer	ISA	National safety authority
Cross Acceptance Safety Case	Manufacturer	ISA	Not relevant
"Top" Safety Case	Infrastructure Manager (IM)	ISA	National safety authority

2.2.5 EN 50159: 2010

The title of the standard reads as “Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems” [20]. Transmission systems, associated with safety-critical parts of a system, are certified in accordance with this standard. EN 50159 classifies three types of transmission systems depending on the type of authorization access from the designer and other external parties. The purpose of the standard is to maintain message properties, such as authenticity, integrity, sequence, and timeliness. The transmission system could face hazardous events from systematic failures, broken wires, cabling errors, antenna misalignment, performance loss, random hardware failure and ageing, human error, maintenance error, electromagnetic interference, cross-talk, thermal noise, fading effects, magnetic storm, fire, earthquake, lightning, etc. The reference architecture for safety-related communication is presented in Figure 6. It illustrates that the safety-related transmission functions are included in the respective safety-related equipment to protect the message properties. The safety-related cryptographic techniques further protect the message by transforming message bits, via an algorithm, into a public or secret key called as the message authentication code. The annexes of the standard are listed in Appendix C.5.

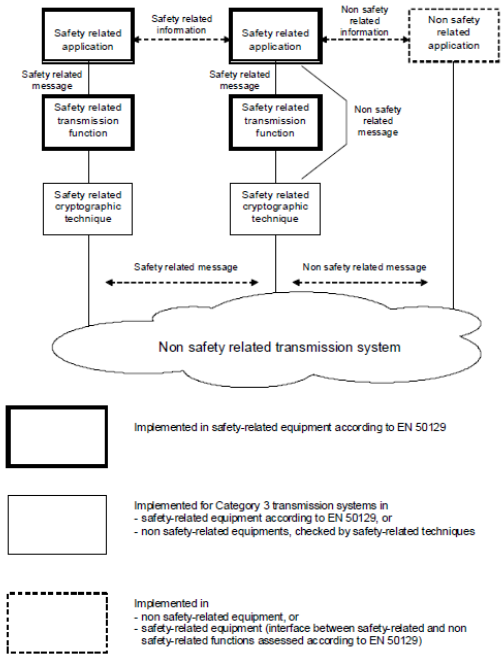

Figure 6: Reference architecture for safety-related communication [20].

2.3 Upcoming Railway Standardization

In the following sections, new standardization protocols commissioned by different governing bodies are discussed. All these initiatives have a common goal of harmonious railway transport across Europe with better safety, higher speed, low life-cycle cost, and an open market.

2.3.1 European Rail Traffic Management System (ERTMS)

In 1989, the EU announced to replace all the 24 national legacy rail signalling and interlocking systems (noted as ATP Class B system) with a single Europe-wide standard system to facilitate interoperability, increased capacity, and safer operation with lesser cost. This system is known as the European Rail Traffic Management System (ERTMS). In 1995, the ERTMS User Group (EUG) was formed with different national railway infrastructure managers. Presently the EUG members include ADIF (Spain), Banedanmark (Denmark), DB (Germany), Jernbaneverket (Norway), Infrabel (Belgium), Network-Rail (UK), ProRail (Netherlands), RFF (France), RFI (Italy), SBB (Switzerland), and Trafikverket (Sweden) [21]. The ERTMS consists of the European Train Control System (ETCS) or ATP Class A system, which substitutes all the ATP Class B systems, and a wireless standard dedicated for railway communications known as Global System for Mobile Communications – Railway (GSM-R). In future, GSM-R could be migrated towards an IP based architecture. The ERTMS system includes on-board (European Vital Computer, Driver Machine Interface, Train Interface, Juridical Recording Unit, Balise Transmission Module, and Odometer) and trackside (Eurobalise, LEU, radio in-fill unit, RBC, and interlocking system) components. Some of these elements are modified from the legacy systems to suit with the ERTMS regulations and some are newly introduced, with the most important one is the RBC.

RBC is a safety-critical device situated between the interlocking system and the on-board European Vital Computer (EVC). Typically an RBC consists of a 2oo3 computer for the conversion of interlocking protocols and other controlling functions [22]. The communication protocol between the RBC and the interlocking system is yet to be finalized. The GSM-R communication (Euroradio) between the RBC and on-board units (OBU) is realized via RBC-OBU interfaces [23]. When a train moves from the area of one RBC to another, the information is handed over through the RBC-RBC safe communication interface via Euroradio [24]. Besides these, there are internal and external communication channels and a diagnostic server.

The ERTMS can be implemented by these following levels [25]:

> Level 1 (L1): This system can be layered on top of the existing legacy system. The movement authorities are gathered from the trackside signals by Eurobalises or Euroloop via LEUs (spot transmission) and relayed to the train-borne EVC for calculating critical information, e.g. maximum permissible speeds and braking curves. GSM-R can optionally be used in L1 via radio in-fill units. Train integrity is maintained by track vacancy detection systems, e.g. track circuits and axle counters.

Level 2 (L2): This system obsoletes the trackside signals and introduces the RBC. The interlocking system gathers all the trackside information from Eurobalises (continuous transmission) and routes it to the RBC which transfers movement authorities for the train through GSM-R. On the other hand, the train sends the statuses back to the interlocking system via RBC. L2 maintains train integrity with similar devices as of with L1.

Level 3 (L3): It is of the same configuration as of L2, with the absence of fixed track circuits and axle counters. The real-time train data is calculated by the on-board EVC via sensors and transmitted back to the RBC. This is an important shift from the fixed block system where the train integrity system reserves a block until the train has gone past it. In L3, the moving block system will be realized to facilitate better train headways. The ERTMS levels are illustrated in Figure 7.

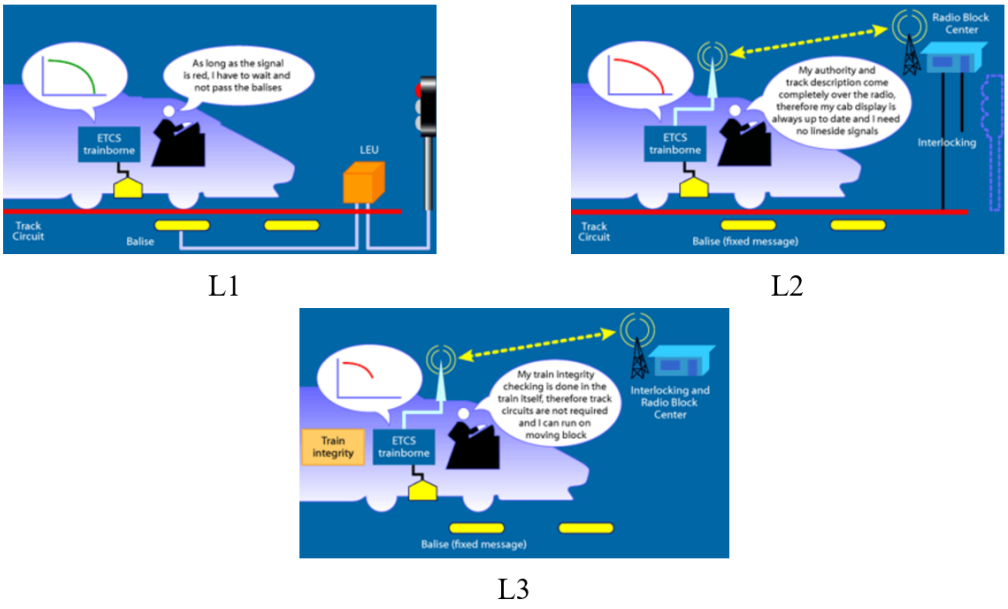

Figure 7: ERTMS levels [26].

Each level has a system requirements specification, known as baselines. A train equipped with ERTMS in one country should be able to run on any track equipped with ERTMS compliant elements worldwide. An ERTMS equipped train can also run on a track equipped with legacy systems, if a Specific Transmission Module (STM) is used as the interface between the EVC and the non-ERTMS interlocking system. In Finland, instead of GSM-R, a new communication mechanism, called as the Future Radio Mobile Communication System (FRMCS) is going to be implemented. It is based on the 5G standards, with an option of further upgradation to 6G [27].

2.3.2 EULYNX

With each step change in railway interlocking technologies, the life-time of the electronic systems are halving and these systems are becoming expired before other legacy equipment. Since the whole setup is supplied primarily by a single supplier, the replacements also come from the same source. Also, installing new technologies in a legacy system requires a new set of interfaces to be introduced which incurs a significant amount of time, cost, and complexity [28]. To tackle this problem and propose standardized control and signalling interfaces, a European consortium, EULYNX was formed by 2014. Presently there are 13 infrastructure managers in the organization from Norway (Bane NOR SF), Luxembourg (CFL), UK (Network Rail), Germany (DB Netz AG), Finland (Väylä), Belgium (Infrabel), Netherlands (ProRail), Italy (RFI), France (SNCF Réseau), Switzerland (SBB), Slovenia (SŽ-I), Sweden (Trafikverket), and Austria (ÖBB) [29]. The present design process in railway interlocking is supported by textual information, schemes, and diagrams. EULYNX aims to replace it with a model-based system engineering (MBSE) approach. Use cases will be built on knowledge, user requirements and other sources, which will be then converted into different SysML models. DB Netze and ProRail along with the Eindhoven University of Technology and Universiteit Twente have developed a formal language and associated tool-set to perform mathematical proofs on the SysML models of the different elements in an interlocking architecture and check whether these models comply with the EULYNX specifications [30].

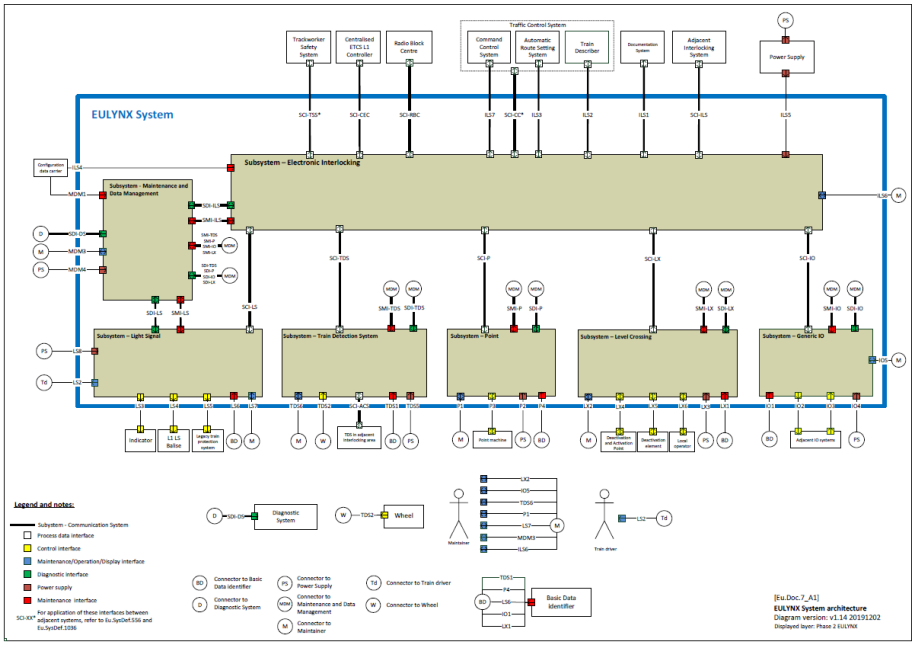

Figure 8: EULYNX System Architecture [31].

The EULYNX system architecture, as depicted in Figure 8, contains subsystems, such as Electronic Interlocking, Light Signal, Point, Generic IO, Train Detection System, Level Crossing, Maintenance and Data Management, and Communication

System. The objective of this system is to modularize the current interlocking system with interfaces which could be interoperably used between the EULYNX member organizations. The system serves the basic railway signalling and interlocking principles, such as route protection, speed supervision, guaranteeing train separation, level crossing protection, maintenance activities, etc. The architecture introduces interfaces, for example between the Electronic Interlocking and other systems, such as RBC (SCI-RBC), TCS (ILS2, 3, 7, SCI-CC), Level Crossing (SCI-LX), Generic IO (SCI-IO), etc. SCI-RBC can be modelled in SysML, since it is supported by a wide range of tools and code generators. Object-oriented languages, e.g. C++ can preferably be used to generate code from this SysML model, because class instances can be used to develop a generic RBC application to suit with different nation-specific applications [32]. In the thesis, different real-time operating systems and development environments have been discussed which allows high-level programming via suitable APIs.

2.3.3 Reference Command and Control Systems Architecture (RCA)

There are different legacy command and control systems (CCS), which include the trackside and on-board elements, installed in different countries around Europe. They are built on different architectures. To implement the visions of ERTMS, various ventures, e.g. Euro Interlocking, INESS, etc. were developed to synchronize these different national CCS. But the EUG came to the conclusion that these projects are of long-term return of investment types. That was the impetus to draw up the formal methods-based reference CCS architecture (RCA) which was established on the ERTMS and EULYNX specifications [33].

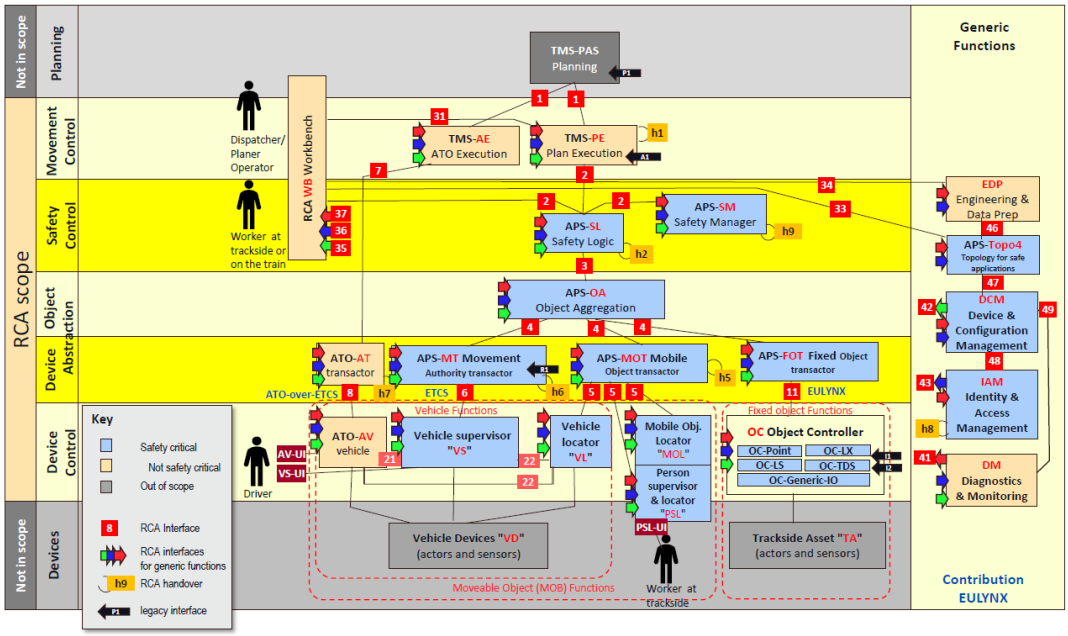

Figure 9: Interface architecture of RCA [34].

The RCA provides an operational plan for the CCS and automatic train operation (ATO) functions between a TMS and trackside objects. A separate initiative named as open CCS on-board reference architecture (OCORA) describes CCS functions for the on-board elements. RCA has gone through several baseline revisions and the present one is RCA gamma which was released in January, 2020. The architecture is presented in Figure 9.

The architecture displays the RCA and legacy interfaces for different safety and non-safety critical components with coloured boxes and arrows. The interlocking system and RBC are split into modular advanced protection system (APS) components, such as "SL" (safety logic), "SM" (safety manager), and "OA" (object aggregation). The SL stores the present state of the trackside elements, train positions, movement authorities, etc. It consists of a risk evaluation mechanism to check if a TMS "PE" (Plan Execution) request will be granted. The SM acts as the watchdog for the whole system by identifying and mitigating hazards, and enforcing a "safe" state. The OA is situated between the SL and the trackside elements which are aggregated as objects. It is used for sending commands from SL to the elements and relaying back the statuses [35]. The RCA advocates for platform independence (PI) by using an RCA PI API as the generalized abstraction. In other safety-critical industries, e.g. avionics, PI is established via partitioning hypervisors as per ARINC 653 specifications. In this thesis, several real-time operating systems with resource partition functionalities are discussed which can be used on COTS target hardware platforms. This could facilitate the RCA PI API to be used as the abstraction layer between interfaces and application logic for code portability and execution of CCS functions as software applications.

3 Present Platform

Mipro TCS-O is the heart of the signalling and interlocking system offered by Mipro Oy which is designed as a generic application. It fulfils safety requirements of the system by conforming to the highest safety capability SIL 4 according to the railway certification standards EN50126, EN50128, and EN50129. Mipro TCS-O consists of the following levels [36]:

Local user interface: It involves a human machine interface (HMI) which is generally used for giving commands to signalling and interlocking system, expressing element statuses, generating alarms, and recording system events to log files.

Communication layer: This is addressed via Ethernet-based TCP/IP communication at the HMI-level and for interlocking communications.

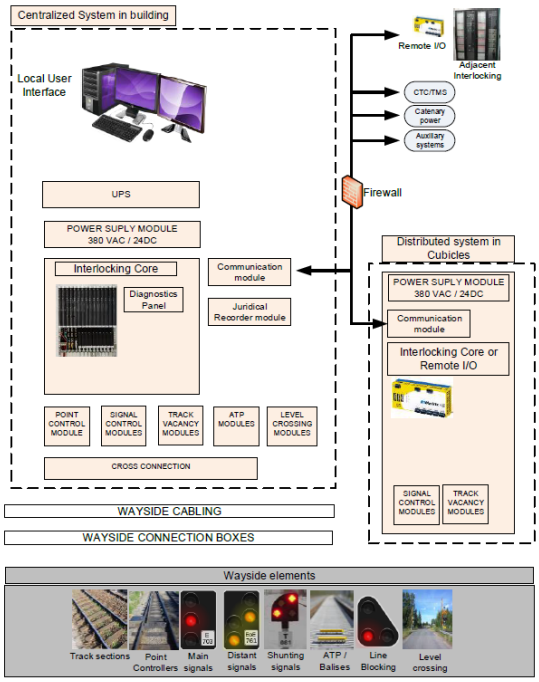

Figure 10: Mipro interlocking and signalling system structure [37].

Mipro TCS-O interlocking layer: It consists of hardware, such as central processing units (CPU), input and output (I/O) modules, communication modules, power supply, uninterruptible power supply (UPS), juridical recorder, etc. along with associated software and interfaces to the trackside elements and auxiliary systems.

Trackside equipment layer: It consists of elements distributed in the trackside, e.g. track sections, point controllers, signals (main, distant, and shunting),

ATP/balises, line blocking, level crossing, etc. This layer execute actions requested by the control system and return statuses to upper hierarchical levels.

The hardware and software elements constituting Mipro TCS-O is supplied by HIMA Paul Hildebrandt GmbH (Brühl, Germany). The following texts are dedicated to illustrate these elements.

3.1 Hardware

Based on the conditions and geographical layout of the application, Mipro TCS-O can be designed as a centralized or distributed configuration. Mipro TCS-O hardware package consists of the following [38]:

System core: It is basically a set of HIMA safety-PLCs consisting of components, such as CPUs, local and remote I/O modules, communication cards, racks and power supplies with internal connections and wiring.

Power supply system: It receives power from an external mains connection and generates power in different voltage levels as required by the modules to perform properly.

Data communication network: This layer is installed in required locations, facilitating different system parts to communicate with each other and external systems through interfaces.

Mounting system: It is the mechanical basis for installing the system core and other components.

Mechanical platform for modules: It is a set of rules and constraints with ready-made design details for allowing fluent development for new functions and their required modules to TCS-O interlocking

Hardware design automation tool: It allows the user to easily configure the hardware of a system based on track element layout and number of elements used in that system.

Juridical recorder: As stated in Chapter 2.1, it is a limited-access tool to record critical functions of interlocking which can be of use in case of different kind of system failures.

Interfaces to external systems: It is used for connecting other interlocking or peripheral systems with Mipro TCS-O. It complies with the supporting communication protocols.

The system core is primarily based on HIMax and HIMatrix product families from HIMA. The hardware products are discussed in the following texts.

3.1.1 HIMax

HIMax is a safety-related modular control system with plug-in modules inserted in base plates for functions, such as processing, input and output, and communication. These base plates are connected with each other via Ethernet cables. HIMax follows HIMA's XMR architecture to guarantee redundancies and fault-tolerance as per the related standards. XMR ensures that in case of a faults or during maintenance activities, affected hardware components can be replaced online. The software fixes for communication protocols, user programs or operating system upgrades can also be done online. This makes the whole system "available for life". The X in "XMR" can take up values from 1 to 4 to suit for different needs [39]. For most of Mipro's applications 2MR or dual modular redundancy is used, meaning there are two CPU modules in the configuration along with dual input and output channels to guarantee process safety and availability. A typical rack structure is presented in Figure 11.

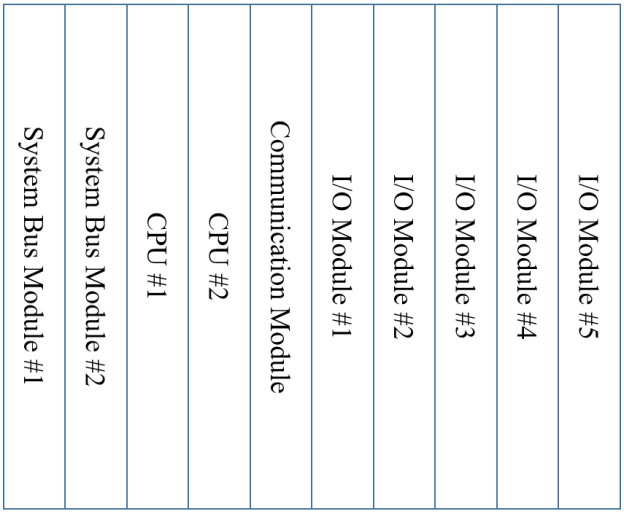

Figure 11: HIMax rack structure.

This system preserves safety by running tests at start-up and during operation in all the components of different modules. During faults, the particular module enters a safe de-energized state. Critical HIMax modules and controller power supplies are duplicated and several time parameters, e.g. process safety time, watchdog time, response time, etc. are monitored [40].

System Bus Module (X-SB): There are two redundant system buses which are used for establishing safe connections between modules, other base plates, and external networks. X-SB manages the module addresses in the System.Rack.Slot (SRS) manner. Each X-SB consists of a 1oo2 safety-related processor system and a system bus controller to communicate with the other system bus, via integrated RJ-45 interfaces [41]. The proprietary operating system from HIMA is loaded into the modules via X-SB.

CPU Module (X-CPU): There are two types of PowerPC-based CPUs available to be used in HIMax system, X-CPU 01 and X-CPU 31. The difference is that the latter is equipped with an integrated system bus and thus the available memory for user programs is lesser [42],[43]. X-CPU 01 is also enabled with better transmission speed. The datasheets are presented in Table B1 of Appendix B.1. The safety certification of HIMax controller is displayed in Figure A1 of Appendix A.1.

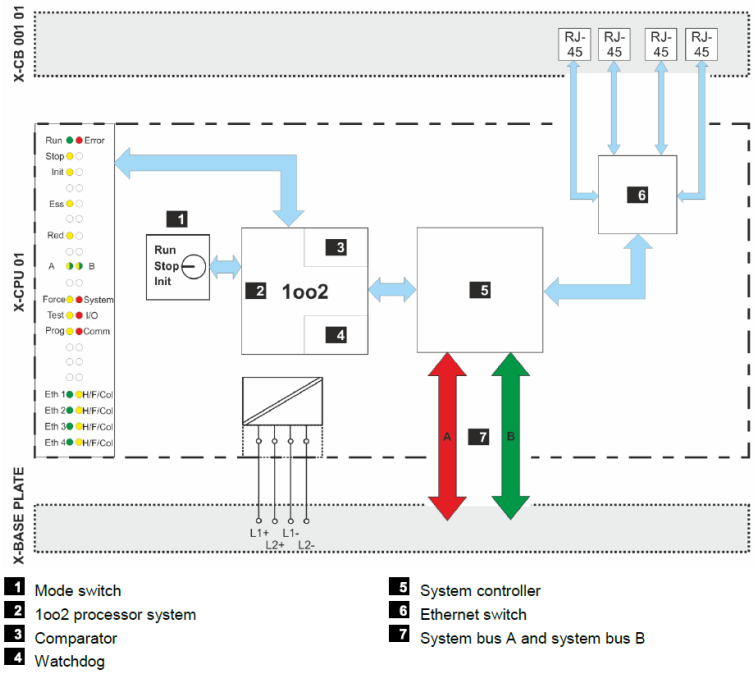

Figure 12: X-CPU 01 block diagram [42].

As depicted in Figure 12, the processor contains two microprocessors with 1oo2 voting mechanism. The process data from both the processors are compared. If the results are the same, then the processors are synchronized. Otherwise, an interrupt is triggered and the module enters the ERROR STOP state. The watchdog constantly checks for the X- CPU health conditions. The non-volatile memory in the module contains the user programs which get transferred into the dedicated program and data memory during booting. The memory also contains the operating system, variables, alarms, events, etc. X-CPU communicates with other CPU modules via Ethernet interfaces with the proprietary safeethernet protocol which will be described in Chapter 3.2.

Communication Module (X-COM): It enables communication with other systems via different interfaces with safeethernet and other industrial protocols. The integrated processor uses the X-SB modules to facilitate data transfer with X-CPU modules. It has 4 RJ-45 Ethernet interfaces with transfer standard 10BASE-T/100BASE-Tx/1000BASE-T and 2 D-sub fieldbus interfaces [44].

I/O Modules: There are different digital input (DI), digital output (DO) and counter input (CI) modules with varying channel capacities are available for use in the HIMax system. These modules are equipped with a safe 1oo2 processor which transfers the information to the X-CPU through X-SB. In case of a fault, the module enters a safe state meaning the input variables of a DI module are reset back to the initial default value (0) and for a DO module, the output channels are de-energized. For CI modules, a safe state is guaranteed by setting the corresponding rotation speed to 0. In the thesis, analog modules from HIMA are not taken into account. The datasheets are presented in Table B2 and B3 of Appendix B.1.

3.1.2 HIMatrix

HIMatrix products are composed systems where a single casing houses a safe processor system, power supply module, and communication and I/O interfaces. Depending on the project requirements, there are different types of HIMatrix modules. A typical system HIMatrix F35 03 is illustrated in Figure 13.

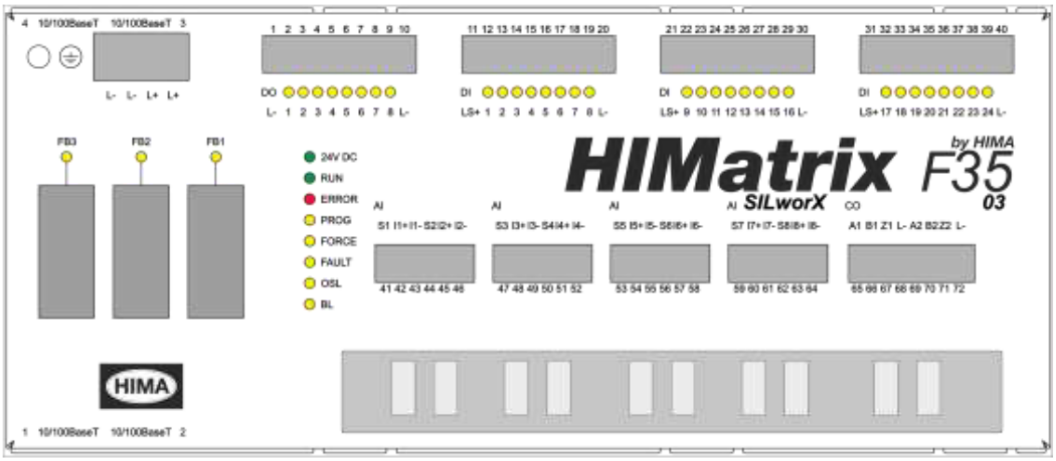

Figure 13: HIMatrix F35 03 rack structure [45].

Like HIMax, HIMatrix is equipped with a processor containing two microprocessors with 1oo2 voting mechanism. There are Ethernet and fieldbus interfaces to connect with the communication protocols. In F35 03, there are 24 DIs, 8 DOs, 8 AIs and 4 CIs [45]. The datasheet of F35 03 is presented in Table B1 of Appendix B.1. Depending on the number of points and signals in a railway project, different HIMatrix solutions, e.g. F31, F30 and F20 can be selected. If the chosen compact system requires more I/O then RIOs, e.g. F1, F2 and F3 can be used. The safety certification of HIMax controller is displayed in Figure A2 of Appendix A.1.

3.2 Communication

Different HIMA systems (HIMax, HIMatrix, remote I/Os etc.) are connected with each other via Ethernet interfaces, following safety protocols. HIMA can communicate with other systems through manufacture-independent and interference-free standard protocols via specific fieldbus submodules. Table 3 represents the list of protocols that can be used for communication.

Table 3: HIMA supported communication protocols [46].

Protocol	SIL	Interfaces
safeethernet	4	Ethernet
Simple Network Time Protocol	No SIL	Ethernet
HIMA X-OPC Server	No SIL	Ethernet
Send/Receive TCP	No SIL	Ethernet
PROFINET IO Controller	No SIL	Ethernet
PROFINET IO Device	No SIL	Ethernet
PROFIsafe Host	3	Ethernet
PROFIsafe F-device	3	Ethernet
PROFIBUS DP Master	No SIL	Fieldbus
PROFIBUS DP Slave	No SIL	Fieldbus
Modbus Master	No SIL	Ethernet
Modbus Slave	No SIL	Ethernet
Synchronous Serial Interface	No SIL	Fieldbus
ComUserTask	No SIL	Ethernet, Fieldbus

The SIL levels are defined as per IEC 61508-2:2010, IEC 61784-3:2019 and EN 50159:2010. Apart from safeethernet, HIMA X-OPC Server and ComUserTask are also provided by HIMA. The Open Platform Communications (OPC) server is run on a third-party system, e.g. a personal computer with Microsoft Windows interface to communicate with HIMA controllers. It follows specifications, such as Data Access (versions 1.0, 2.05a and 3.0) and Alarms&Events (version 1.10) [47]. Users can develop non-safety-critical applications in C programming language and then integrate them into a HIMA system with X-COM module of HIMax or the Ethernet/fieldbus port of HIMatrix via the proprietary ComUserTask protocol. The specific C program cycle time is different from the CPU cycle time and it does not interfere with the safe applications. The concerned development environment is based on GNU C compiler and Cygwin [48].

A safety-critical system demands that the safe and non-safe data must be transmitted over a single standard network. But it was a riddle to solve in the past decades, as the reaction time for a change in the safety-related variable is required to be lesser than that of a non-safe one [49]. HIMA's safeethernet protocol uses unsafe data transfer channels (Ethernet) in accordance with the black channel approach and monitors the messages on the transmitter and receiver side by using safety-related protocol mechanism. This allows the user to rely on normal Ethernet network components,

such as hubs, switches, routers, etc. within a safety-related network. Also, security and real-time ability associated with standard Ethernet are achievable. This protocol ensures deterministic behaviour in the presence of faults. The system automatically integrates new components in the running system. All network components can be replaced during operation. Ethernet is thus real-time capable with a possible transfer speed of up to 1 GBit/s for safety-related data. Redundant safeethernet connection between different controllers is established via a network based on ring topology. Parameters, such as receive timeout, expected response time, worst-case response time, etc. are used to check whether the network satisfies the safety conditions. These parameters are also used for selecting various safeethernet profiles (fast & cleanroom, fast & noisy, slow & noisy etc.) to optimize data throughput. Different communication medium, such as Ethernet patch cables (Cat. 5e), CAN, RS-485, PROFINET cables are used to satisfy corresponding protocols. The connections can be established by cables with a minimum cross-section of 0.2 mm^2 [46].

3.3 Software

Each HIMA controller is equipped with a proprietary operating system (OS) which executes user programs written in the SILworX programming tool. The OS reads the input data, processes the logic function and cyclically writes the output data. It also performs tasks, e.g. comprehensive self-tests of the modules during start-up and in operation, input and output testing during operation, data transmission, and fault diagnoses. HIMA releases versions of the OS marked by the revision number and the cyclic redundancy check (CRC) signatures. A new version can be updated online [40]. SILworX can be used the integrated development environment (IDE) for the proprietary OS version 7 and higher. For the prior versions, another HIMA IDE, ELOP II Factory can be used. There are hardlock (USB dongle) and softlock licenses available for SILworX. Hardlock licenses can be used on any personal computer but the softlock license is bound to a specific one. Depending on the requirements, there are license variants, e.g. full license (for any HIMA system), HIMatrix license (for HIMatrix and remote I/Os) and maintenance license (for any HIMA system with read-only access) [50].

The screen layout of a SILworX environment is depicted in Figure 14. It has all the familiar setup of an automation development platform including, the menu and symbol bars which showcase the buttons for opening, editing, deploying of a project; the structure tree which illustrates all the elements of a specific SILworX project, such as variables, the hardware used, library, code, license management, etc.; the vertical action bar for editing, verifying, going online/offline, code generation, etc., and the workspace which contains a program drawing area, object panel and navigation panel. There is a logbook for registering important operating steps, code generation and verification results. SILworX allows the use global variables for storing the input and output values of a hardware resource, and exchanging data in a particular user program and with the external systems. Local variables are used only inside a particular program organisation unit (POU).

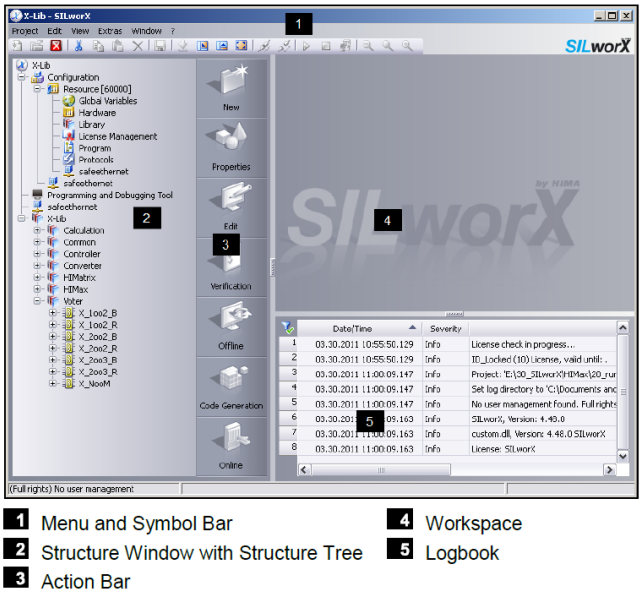

Figure 14: Screen layout of SILworX [50].

Programming languages listed in IEC 61131-3 can be used for developing user applications in SILworX. The IDE also allows usage of C++ function blocks with the generic SILworX functional blocks. The licenses for creating and modifying the C++ programs comes as a separate package. The input and output variables of the C++ function blocks can serve as an interface to the functions of the C++ source code from other third-party tools. But the C++ source code cannot be tested online or simulated offline and it can be used for safety-related applications only after consultation with the testing authority responsible for the final inspection [51]. The safety certifications of SILworX are displayed in Figure A3 and A4 of Appendix A.1.

4 Thesis Methodology

This chapter presents the hardware, OS, and IDEs investigated in the thesis to build an alternative platform. These products are chosen based on the following conditions that the solutions must be

1. of COTS type and pre-certified to the highest levels of safety concerning the generic industrial standard (IEC 61508) and rail specific standards (EN 5012x) to save time and money, and

2. open in a sense that if in future, for example, a new OS is needed to be installed then the hardware and IDE must be compatible with that change.

For the thesis, the following products are explored: Hardware: ControlSafe Platform (SMART Embedded Computing) and MH50C (MEN Mikro Elektronik GmbH). OS: VxWorks 7 (Wind River Systems), QNX OS for Safety (BlackBerry Limited), INTEGRITY (Green Hills Software), and PikeOS (SYSGO GmbH). IDE: SCADE (Ansys, Inc.), FlexiSafe (infoteam Software AG), Prover Trident (Prover Technology AB), and CODESYS Safety (3S-Smart Software Solutions GmbH). These products can give 32 possible combinations for an alternative platform as shown in Figure 15.

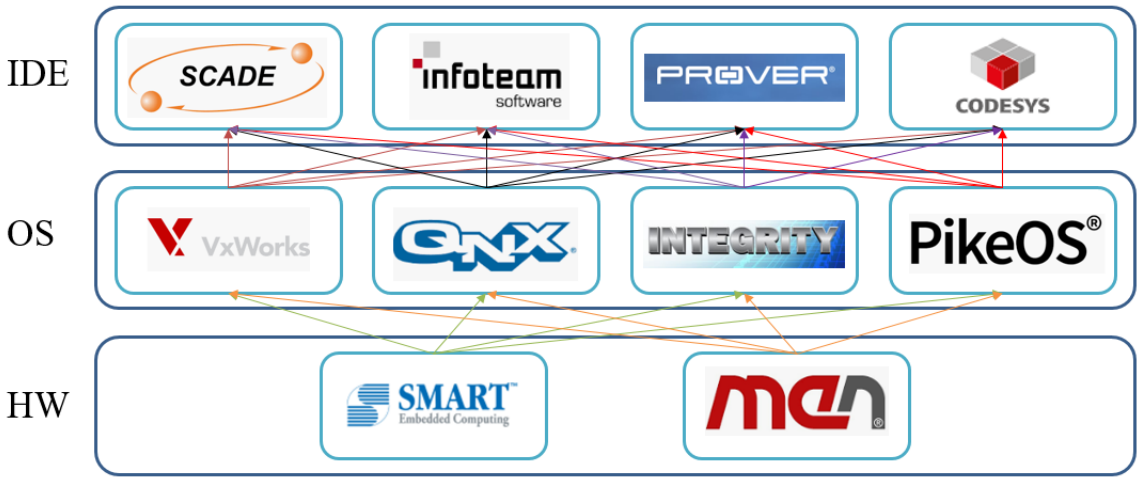

Figure 15: Possible combinations of hardware, OS, and IDEs.

A particular combination is quantified with a performance index or cost symbolized as, $C_i(H_j, O_k, E_l)$, where $i = 1...32, j = 1, 2, k = 1...4, l = 1...4$, which is constituted of the following costs:

1. standalone hardware cost: $C(H_j)$,

2. standalone OS cost: $C(O_k)$,

3. standalone IDE cost: $C(E_l)$,

4. compatibility costs: $C(H_j, O_k)$ and $C(O_k, E_l)$.

The first three costs signify the individual merits of the hardware, OS, and IDE platforms. The compatibility cost indicates the affinity of a hardware platform and an IDE with a specific OS. The whole platform is assumed to be a linear system, thus the superposition principle has been adopted to calculate the final cost which is the summation of all the other costs:

$$C_i(H_j, O_k, E_l) = C(H_j) + C(O_k) + C(E_l) + C(H_j, O_k) + C(O_k, E_l)$$

These constituent costs are based on the certain parameters, e.g. $C(H_j)$ depends on the hardware architecture, I/O capacity, certifications, operating temperature, etc.; $C(O_k)$ depends on kernel architecture, scheduling policies, support for target architectures, etc.; $C(E_l)$ depends on the framework, supporting languages, development tools, etc. Chapter 8 discusses these parameters in detail.

Not all the parameters hold equal significance while choosing for a particular product, e.g. availability of all the required certifications for a hardware platform is more important than the range of the operating temperatures. Because the money and effort spent to certify a component are higher than installing additional heating or cooling arrangements. The critical factors are allocated with a weightage of 1 and the others are with 0.5. Based on the datasheets presented in Appendix B, every parameter of each product is assigned with a score in the scale of 1 to 5. The respective costs are calculated by multiplying the weightage with the score as presented in Chapter 8.

5 Alternative Hardware Platforms

Railway interlocking employs a hardware platform or a PLC which is "safer" than the standard PLCs. A safe PLC for any safety-critical system adheres to the regulations set by IEC 61508. A safe PLC for railways further follows the industry-specific standards EN 50126, EN 50128, and EN 50129 which are described in Chapter 2.2. In Europe, there are several product certification services offered by organisations, such as TÜV Rheinland, TÜV Nord, TÜV SÜD, Exida, etc. A safe PLC differs from a standard one in terms of architecture, inputs, and outputs [52]. From the architectural point of view, the safe PLC is equipped with two microprocessors to guarantee redundancy. RAM and flash memories, used for storing and executing of control programs, are protected and monitored by special-purpose circuits. For a safe PLC, the functionalities of the input channels are further secured by an additional internal 'output' circuit. A standard PLC's output channel is equipped with a switching device. But for a safe PLC, there are two such devices, which are controlled by unique microprocessors. This preserves system integrity by driving an output channel to a known "safe" state in case there is a failure in the microprocessors or devices. Because of these redundancy and self-testing features, a safe PLC generally costs 25% to 30% more than that of a standard PLC. In the following sections, the hardware selections described in Chapter 4 will be briefly introduced.

5.1 ControlSafe Platform (CSP)

It was originally developed by Artesyn Embedded Computing (Tempe, Arizona, USA) which was a spinoff from the Emerson EC group (Motorola, Force Computers and Astec). Artesyn was acquired by SMART Global Holdings in July 2019, changing the name to SMART Embedded Computing (SMART EC) [53]. The rack structure is of the CSP is presented in Figure 16.

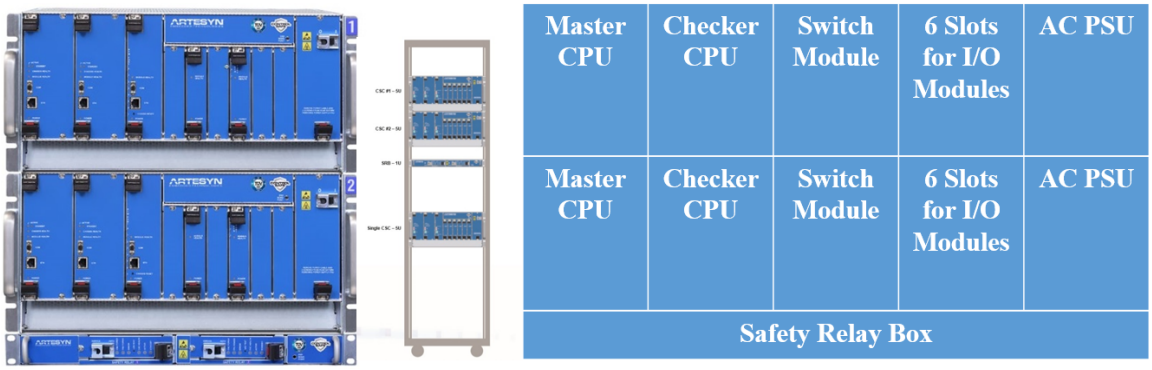

Figure 16: Front-view of the ControlSafe Platform [54].

Each rack consists of two CPUs (Master and Checker), a switch module with 10/100/1000 BASE-T Ethernet ports to interface with other modules, and six I/O modules along with an AC power supply unit. Each rack is called as ControlSafe Computer (CSC). The Safety Relay Box (SRB) is used for evaluating which CSC

is operating and which one is in standby mode. The CSP has identical processor architecture, as each CPU module has one NXP QorIQ P2 processor while the I/O module has one NXP QorIQ P1 processor.

In railway systems, most of the processors use hard lockstep synchronization technique where firstly the clocks of both the redundant processors are synchronized, then the processors execute the same instructions at the same time and finally the data and address bits from both execution results are compared. If they are same then these results will drive the specific external equipment, else the system will fail safely. The requirement for the processors to execute the same instructions at the same time requires the processors to be deterministic. This condition is hard to achieve as modern multi-threaded processors are not strictly deterministic due to various reasons, e.g., soft errors, modern power management methods, cache misses, etc. Secondly, due to the non-deterministic jitters produced by clock multipliers and multi-channel memory architecture, it is practically impossible to synchronize the data buses of two different CPUs.

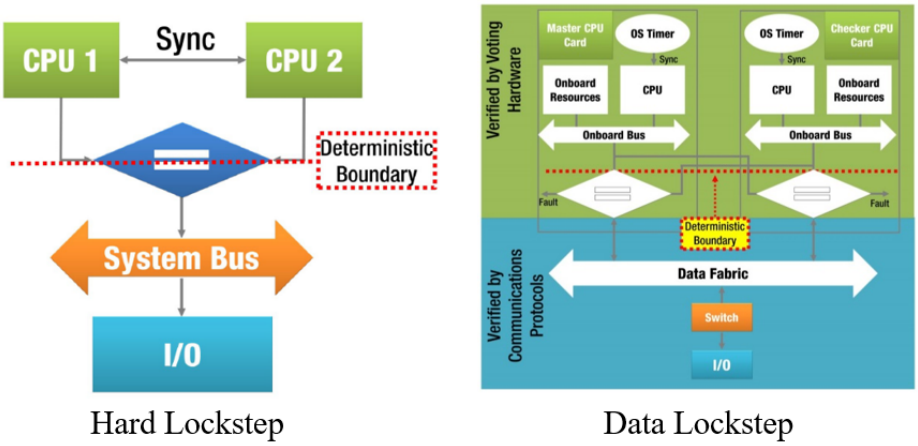

Figure 17: Hard and data lockstep architectures [55].

SMART EC has come up with a solution called as data lockstep architecture [55]. Whereas the hard lockstep sets the deterministic boundary at the processor itself, for data lockstep it is at the output stage of the processor board and to the system data fabric. As shown in Figure 17, the data and address bits are compared before arriving at the data bus. This also allows to upgrade the processor architecture over time while retaining the same I/Os.

CSP employs a 2oo2 voting scheme with the Master and Checker CPUs, and dual redundancy with two CSCs. At one time, one of the CSCs can be operational. The user application running on the "active" CSC has full control over the I/O ports. The same application running on the "standby" CSC monitors safety-relevant input ports and all interference-free ports, but by default cannot drive any safety-relevant output. To designate the active/standby statuses for the CSCs, a hardware-based mechanism called the Safety Relay Box (SRB) is used. The SRB contains two safety relay-based field-replaceable units (FRU), each of which is connected to one CSC. After the SRB's power is turned on, it selects the first CSC for which both the CPUs

are healthy to be the active CSC. The other CSC enters the standby mode. Upon detecting a failure, the active CSC signals its state to the SRB, which in turn hands over the authority to drive the safety-relevant outputs to the standby CSC, provided it is healthy. SMART EC also gives a provision to use a patented software measure, Direct Connect Algorithm (DCA), which can be used instead of SRB to reduce hardware hassles. The datasheet of the CSP is presented in Table B4 of Appendix B.2.

Different types I/O modules can be integrated into the CSP, e.g. the general-purpose I/O module, built on ARM Cortex with Altera FPGA SoC, with 16 channels for DI, DO and CI [56]; CAN module, built on NXP QorIQ P1 processor, with 4 ports to connect with trackside devices or external systems [57]; and UART module, built on ARM Cortex with Altera FPGA SoC, with 6 serial interfaces for RS485/RS422/RS232 [58]. Additional Ethernet modules, equipped with 2 ports of 10/100/1000 BASE-T capabilities, can be inserted in the I/O slots to increase connectivity [59]. Apart from the CSP, SMART EC offers different other platforms, which are based on the same architecture but with varying footprints, e.g., Expansion Box Platform, with 11 I/O modules, for larger interlocking applications [60], and Carborne Platform, with a DC-powered compact chassis and 12 I/O modules [61], for on-board applications, e.g. ATP, ATO etc.

SMART EC has described CSP as a system where the ControlSafe Software, based on Wind River's VxWorks 653 operating system, works on top of the respective CSCs. This whole package is certified as per EN 50126: 1999 (SIL4), EN 50129: 2003 (SIL4), EN 50128: 2011 (SIL4), IEC 61508-1(ed.2) (SIL3), IEC 61508-2(ed.2) (SIL3) and IEC 61508-3(ed.2) (SIL3). The safety certification is displayed in Figure A5 in Appendix A.2. The certification parameters include safe application programming, voting and 2oo2 active/standby arbitration, and safety-related communication [62]. The other platforms are also certified to the highest safety standards [153], [154]. The SMART EC package for a certain project includes, the required platform/s, runtime license, board support packages (BSP) for VxWorks, and API libraries. The certification evidence package contains safety cases, safety manuals, SAR, and SIL4 safety certificates from TÜV SÜD. SMART EC promises 15 years of planned product life and 25 years of extended support and services. The hardware is designed to deliver platform hardware availability of six nines (99.9999%) [54]. SMART EC has strong strategic partnerships with key silicon and software vendors, such as NXP/Freescale and Wind River for obsolescence and inventory management. Besides these, SMART EC provides technical support regarding application porting, development consulting, engineering, installation, repair, root cause analysis, revision management, migration from legacy system to a new product generation, etc. [63].

CSP has been used in collaboration with China Railway Signal & Communication (CRSC Wanquan, China) for a 10 station interlocking application for a power plant coal transportation system in Pakistan, and a tram point controller application, with custom I/O modules, for Hainan Sanya Rail Transit Project in China [64]. The Expansion Box Platform was used for a 65.7 km long track covering six stations in South Korea for Hyukshin Engineering Company Limited (South Korea) [65]. All the applications have successfully met the SIL4 criteria.

5.2 MH50C

MH50C or menTCS platform is developed by MEN Mikro Elektronik GmbH (Nürnberg, Germany) which was merged with the Swiss communication company duagon Holding AG in April, 2019 [66]. The rack structure is presented in Figure 18.

Figure 18: Front-view of MH50C [67].

It is a 40 HP CompactPCI system configured with a safe CPU, a real-time Ethernet card, I/O slots, and a power supply unit. Figure 19 depicts the typical rack structure of MEN MH50C Platform [67]. There are three Intel Atom-based processors in the single CPU module (F75P), as illustrated in Figure 19. Out of these three, 2 are control processors (CP) and the other one is I/O processor (IOP) [68]. The CPs facilitate flexible implementation options for functional safety requirements and provide support for advanced, certified operating systems up to SIL4 by asserting a "safe domain". These are configured for deterministic behaviour with techniques e.g., hyper-threading speed-step and basic input/output system (BIOS) interrupts being disabled.

The IOP lies outside of the safe domain, looks after the common I/O and memory facilities, and provides a user-friendly software interface. The Inter-Communication FPGA (ICOM) provides communication between all three processors via on-board Ethernet of 100BASE-T capabilities or shared RAM. F75P enters a specific "fail-silent" safe state after each failure and restarts automatically. There is an independent supervisor which acts as a timeout watchdog to check for over-voltage, under-voltage, excess temperature, and internal errors of the CPs and ICOM. The function is implemented in the IOP by a dedicated Board Management Controller (BMC). The records of these malfunctions are stored in a non-volatile FRAM. There is also a real-time clock with super-capacitor backup connected with the IOP. Each processor has been allotted with caches, flash memory and RAM. In addition, the IOP can be attached with mass storage devices for boot image and file system. For synchronization, a software-based proprietary function (SyncLayer) is used to ensure

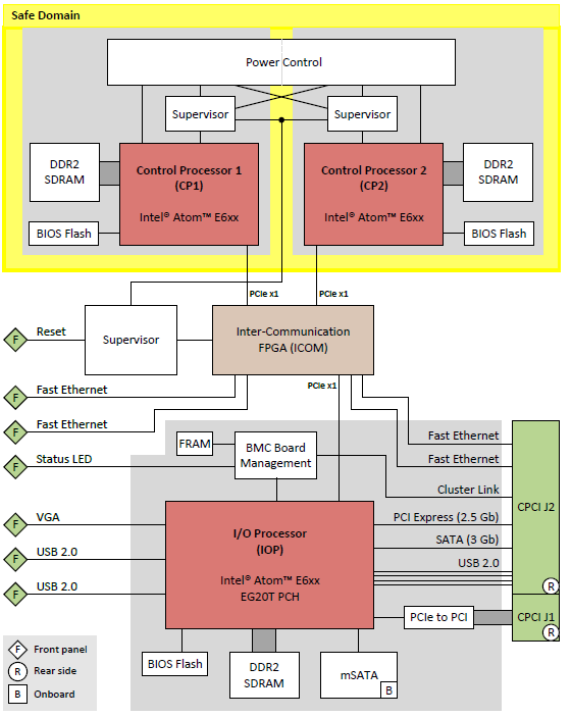

Figure 19: F75P architecture [68].

both CPs use the same input data and verify matching of the calculated output data.

For safe communication between the F75P and the I/O modules, a black channel approach along with EN 50159 certified FailSafe over EtherCAT (FSoE) is used, which begins at the boundaries of the safe domain on the F75P board. EtherCAT is a real-time Industrial Ethernet technology introduced by Beckhoff Automation in 2003. In this communication mechanism, the master sends a telegram that passes through each slave in the network. The nodes read the data "on the fly" and insert their own data in the frame. FSoE uses frames called as safety containers, which contain safety-critical process data and security measures. The containers along with non-safety critical data are transferred over the untrusted black channel [69]. For F75P, the IOP takes safe containers from both the CPs which include process and communication data (header, CRC etc.), and generates EtherCAT messages. Any error caused by the IOP is detected by the safety communication layer. EtherCAT is a deterministic protocol which operates without any network switches, with cycle times less than 5 ms. EtherCAT supports a ring topology which provides a continuity in service in case of a broken cable or the loss of power on a particular remote I/O panel [70]. MEN Mikro's proprietary Process Data Application Framework (PACY) is integrated with FSoE protocol. PACY acts as an abstraction layer to handle the communication between CPU, I/O modules and user programs. It is a C library which provides an API for application developers to control and monitor different kinds of I/O through C programming language variables. Every I/O channel is represented by a specific independent PACY channel [71].

MEN Mikro offers a DI module with 16 channels [72] and DO modules with 8

channels, with different output types, such as load to ground (high-side switching) [73] and load to supply voltage (low-side switching) [74]. To achieve the highest levels of safety integrity (SIL 4), two channels of a module is used for a single I/O. These modules satisfy safety functionalities through measures, such as local over-voltage or under-voltage and over-temperature monitoring, external supply voltage supervision, self-test mechanisms in every 10 ms via PACY, clock monitoring, and safe communication through FSoE. In case of fatal errors, the module drives the respective channel/s to safe state within 10 ms. There are remote I/O modules with 4 and 8 slots available to be connected with MH50C via FSoE to integrate applications, such as train communication network with different regional TCS configurations [75].

MEN Mikro has certified the safety-related programmable system F75P-3U Safe Computer via TÜV SÜD as per EN 50126: 1999 (SIL4), EN 50129: 2003 (SIL4), IEC 61508-1(ed.2) (SIL1-3), IEC 61508-2(ed.2) (SIL1-3). Apart from that, MEN Mikro has collaborated with Blackberry to develop a BSP for F75P which is based on QNX OS for Safety. This bundle also got certified according to EN 50128: 2011 (SIL4), IEC 61508-3(ed.2) (SIL3). The synchronization mechanism SyncLayer and the safe API for QNX, named as Y-COM, are certified as per EN 50128: 2011 (SIL4) and IEC 61508-3: 2010 (SIL3) [76], [77]. MEN Mikro offers two different packages. In the first one, only the F75P is offered along with safety case, safety user guide, certificates, and assessment report. And the other is a bundled package including QNX BSP along with the previously mentioned contents. MEN Mikro provides 40 hours of support with the F75P standalone package and 90 hours of extensive support for the bundled package. The company also promises to deliver identical boards per project for 10 years along with 25 years of technical support per project [71], [78]. The datasheet of MH50C is presented in Table B5 of Appendix B.3.

MEN Mikro has extensive partnerships with a range of companies in the embedded and railway industries, such as NXP Semiconductors N.V., Wind River Systems, Green Hills Software, SYSGO GmbH, Intel Corporation, BlackBerry Limited, infoteam Software AG, etc. [79]. The MH50C has been used in various wayside and rolling stock applications including, interlocking, level crossings, ATO, ATP, CBTC, etc., but none of these are published in the public domain.

6 Alternative Operating System Platforms

A general purpose OS is a program that acts as an intermediary between the user and the computer hardware. It performs three main functions, such as managing the computer's resources, e.g. CPU, disk drives, and printers etc.; establishing a user interface; and executing and providing services for the application software [80]. Depending on the schedulers that decide which program to execute by rationing system resources, there are different types of OS, e.g. UNIX distributes each user a sufficient processing time but Windows ensures that the user request is served as soon as possible. For a safety-critical system, the importance of performing certain activities are of paramount importance. This might require pausing the general applications and commencing a higher priority task. This calls for a special purpose, real-time operating system (RTOS) which serves real-time applications to meet critical deadlines by switching between tasks based on their priorities (event-driven) or clock interrupts (time-sharing). Most of the RTOS adopt the microkernel architecture where the vital services, e.g. inter process-communication, memory management, and CPU scheduling are kept inside the kernel space and other services, e.g. user application, file system, networking drivers, etc. are placed in different address spaces. The limited "micro" size of the kernel increases the execution speed of critical services, protects it from getting corrupted, and enables other services to get installed easily. For an RTOS, the preemptive priority scheduling is one of the most popular scheduling algorithms. It assigns each task with a priority. If a higher priority task lines up in the queue, the ongoing task can be pre-empted. Some RTOS follow round-robin scheduling where tasks are given a quantum of CPU time. Each task is meant to run only in their respective quantum and will be halted after that, regardless of its progress. In the following texts, the thesis will briefly cover the COTS RTOS platforms mentioned in Chapter 4.

6.1 VxWorks 7

It is released and maintained by Wind River Systems (California, USA), which was acquired by Texas Pacific Group from Intel on 2018. The legacy VxWorks OS is one of the most deployed RTOS with applications ranging from industrial sectors to NASA missions [81]. The kernel of VxWorks 7, an RTOS for safety-critical railway and automotive applications, is based on VxWorks 653 which was designed to serve aeronautic purposes. It is of a microkernel architecture which permits preemptive priority-based and round-robin scheduling with message passing type of inter-process communication (IPC). VxWorks 7 allows up to 255 partitions to integrate applications of different safety-criticality in one platform with easy portability of other VxWorks applications. It is also supported with Wind River's IEC 61508 (SIL 3) Helix Virtualization Platform. VxWorks 7 provides BSPs with multi-processing support for over 80 boards from different architectures, such as Arm, PowerPC, Intel, RISC-V, etc. It allows the end-users to choose from different APIs to avail open standards for writing applications in Ada, Java, C and C++ [82]. This RTOS is certified with SIL 3 as per the first, third and fourth part of IEC 61508:

2010 [83]. The safety certification is displayed in Figure A6 in Appendix A.3. Wind River chooses to opt for railway certifications only with specific hardware platforms, e.g. with CSP from SMART EC, as illustrated in Chapter 5.1.

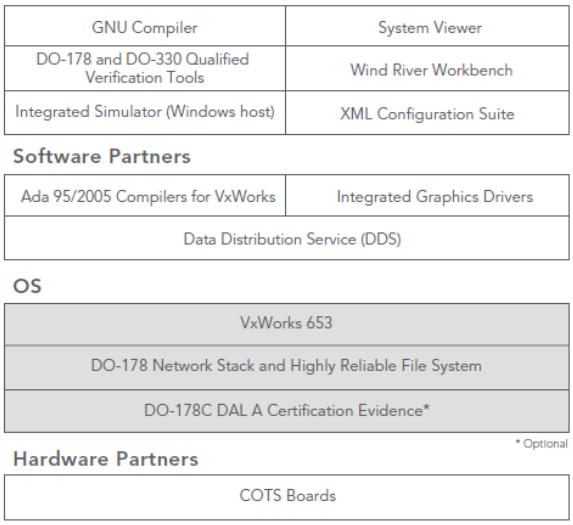

Figure 20: Wind River VxWorks 653 Platform [84].

VxWorks 7 is packed with a proprietary development environment, Workbench, which is based on Eclipse framework. In this IDE, applications can be developed with high-level programming languages, e.g. C or C++ [85]. The proprietary DIAB compiler toolchain fulfils the requirements for T3 tools as per IEC 61508-3 [86]. The safety certification is displayed in Figure A7 in Appendix A.3. There are options to use other compilers, e.g. LLVM for Arm and Intel architectures, and GCC for PowerPC architecture. The IDE uses its own debugger for codes running simultaneously on multiple cores, tasks, physical processors, and other target OS. It is based on on-chip-debugging for easier integration of new hardware designs. Workbench can be hosted on Windows, Ubuntu, Red Hat, and others. It contains analysis tools, such as System Viewer for providing a graphical representation about how tasks, threads, interrupts, etc. are getting executed on the target; Performance Profiler which reports on how much CPU cycles are being consumed in a program by individual routines; Memory Analyzer for tracking memory usage and detecting memory leaks via system calls or third-party libraries; Data Monitor for checking variables and data structures; and Code Coverage Analyzer which looks into which code segments are executed during testing and removes unused codes. The datasheet of the RTOS and IDE is presented in Table B6 of Appendix B.4.

VxWorks 7 and its toolchain have been used for a CBTC development project of Beijing Traffic Control Technology Co., Ltd (China). The application was about developing an automatic control system that can handle traffic headway of 90 seconds in the Yizhuang and Changping lines of the Beijing subway network [87]. VxWorks 7 has been installed in the world's first Wi-Fi and LTE based SIL 4 certified CBTC system, Korean Radio-based Train Control System (South Korea). A custom BSP was made in collaboration with the customer LS Electric (South Korea) and other

services were provided [88].

6.2 QNX OS for Safety (QOS)

QNX is one of the prominent suppliers of RTOS for the last four decades. Their legacy line of products are used in automotive, medical, robotic, defence, industrial, and transportation applications. In 2010, QNX Software Systems was acquired by BlackBerry/RIM (Canada) [89]. The railway specific RTOS is named as QNX OS for Safety (QOS). It is a safety-certified version of the popular microkernel-based QNX Neutrino RTOS architecture, which supports spatial and temporal domain separation at the application level. QOS allows tasks of mixed criticalities to be used in the same platform without any interferences [90]. Along with the message passing type of IPC, QOS allows for preemptive priority-based scheduling with the option to use other methods, distributed priority inheritance, and adaptive partitioning. There are BSPs available to comply with boards from AMD, Intel, NVIDIA, NXP, Qualcomm, Renesas, Samsung, TI, Xilinx SoCs, etc. QOS supports a broad range of POSIX APIs. Security is guaranteed by mechanisms, such as secure boot, integrity measurement, sandboxing, access control (mandatory or discretionary), and rootless execution [91]. QOS is certified to SIL 3 as per IEC 61508 [92]. The railway certifications are done only with specific hardware platforms, e.g. MH50C from MEN, as illustrated in Chapter 5.2. Blackberry offers the IEC 61508 (SIL 3) certified QNX Hypervisor for Safety upon which a guest OS, e.g. QOS can be run. This environment allows the guest OS to pin virtual CPUs on cores from different hardware manufacturers [93]. The safety certification is displayed in Figure A9 in Appendix A.4.

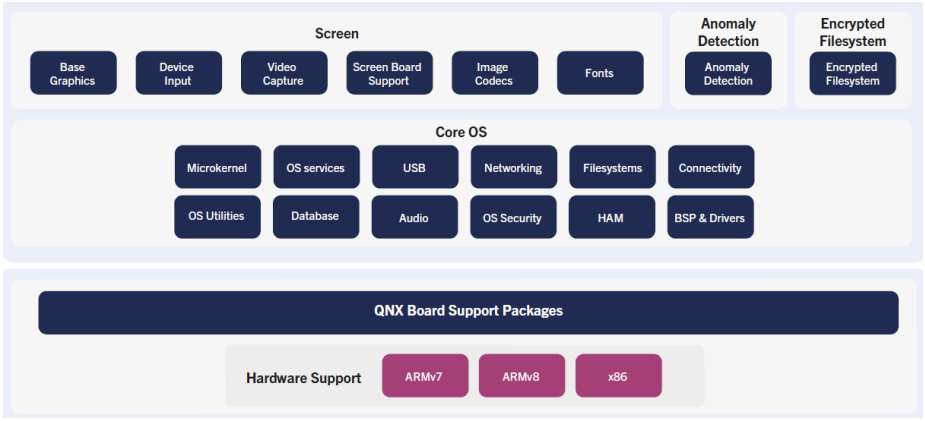

Figure 21: QNX Neutrino RTOS architecture [91].

QOS has an integrated IDE, QNX Momentics Tool Suite which is based on Eclipse framework and supports C, C++, Python, Perl, etc. The toolchain is equipped with the generic GCC compiler and GDB debugger. The analysis tools include, System Profiler to monitor OS events, e.g. kernel calls, interrupts, etc.; Code Coverage to enable a user to decide which parts of the program to run, and which parts need further testing; specific tools to check for race conditions, memory leaks, security issues etc. during testing phases; Valgrind for runtime error detection etc. The IDE

has a special advantage due to the ability its host macOS, apart from Windows and Linux [94]. It fulfills the requirements for T3 tools as per IEC 61508-3 [92]. The combined safety certification of QOS and Momentics is displayed in Figure A8 in Appendix A.4. The rail specific applications of QOS are not available in the public domain. QOS datasheet is presented in Table B7 of Appendix B.5.

6.3 INTEGRITY

INTEGRITY is an RTOS developed by Green Hills Software LLC (California, USA). It is the leading supplier of RTOS in the American defence sector for the last 40 years [95]. The RTOS is based on a separation supported microkernel with a real-time scheduler allowing multiple priority levels. INTEGRITY uses message passing type of IPC. The partitions are well secured from unauthorized accesses which can lead to denial-of-service attacks. The kernel never blocks interrupts, so that highest priority interrupts can be processed with minimum latency. Messages, semaphores and other kernel objects created during process requests are kept in process memory, instead of kernel memory. INTEGRITY has subsided the kernel with a memory stack, to prevent the overflow of the user stack. It supports multiprocessing with a range of target hardware from Altera, ARM, AMD, Fujitsu, IBM, PowerPC, NXP, Renesas, TI, Xilinx etc. There is a hypervisor platform, INTEGRITY Multivisor, available with hardware-assisted virtualization technologies for architectures, such as ARM -VE, Intel VT-x and VT-d, and virtualization-enabled PowerPC. If the target hardware is lacking hypervisor assistance, INTEGRITY Multivisor is able to modify the guest OS to enhance performance [96]. The RTOS is certified to SIL 3 as per IEC 61508: 2010 [97] and SIL3/4 as per EN 50128: 2011 [98]. The respective safety certifications are displayed in Figure A10 and A11 of A.5.

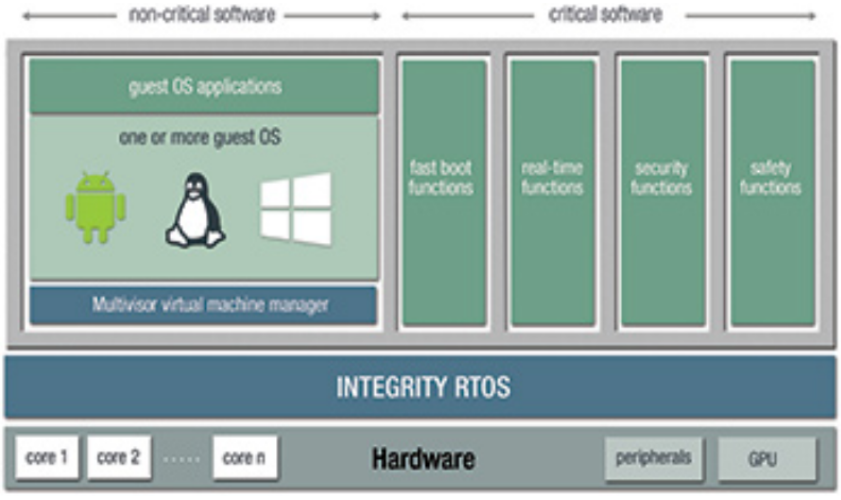

Figure 22: INTEGRITY Multivisor [96].

MULTI IDE is the proprietary development platform supplied by Green Hills Software. It is packed with a proprietary compiler and debugger. The IDE supports C, C++, EC++, and Ada programming languages. There are analysis tools, such as

TimeMachine and PathAnalyzer which provide a time-based view of every function executed in the program and monitor if the code is diverting from the expected path; DoubleCheck for tracking down bugs before running on a simulator; EventAnalyzer for displaying time-consuming processes and optimization; Memory Allocation for checking memory leaks, etc. The IDE can be hosted on Windows and Linux and the code can be ported to different hardware architectures, e.g. ARM, PowerPC and Intel [99]. MULTI IDE toolchain along with run-time libraries meet the requirements for T3 tools as per IEC 61508-3: 2010 and also certified as SIL 4 according to EN 50128: 2011 [100]. The safety certification is displayed in Figure A12 in Appendix A.5. INTEGRITY RTOS and the associated toolchain have been used for Train Control Management System of Bombardier Inc. (Canada); RBC and interlocking platforms manufactured by Sirti S.p.A. (Italy); and EVC system designed by CAF (Spain) [101]. INTEGRITY datasheet is presented in Table B8 of Appendix B.6.

6.4 PikeOS

It is developed by SYSGO GmbH (Mainz, Germany), a subsidiary of the Thales group since 2012. PikeOS is in use for the last three decades in more than 100 million embedded devices [102]. Like the previous RTOS platforms, PikeOS is based on separation microkernel architecture to prevent the propagation of faults. The applications are further secured via communication encryption and binary verification. The RTOS is packed with a preemptive priority-based scheduler and a message-passing type of IPC. Multiprocessing is supported with processor families from PowerPC, x86, ARM, Sparc V8/LEON, etc. PikeOS Hypervisor enacts a hypervisor-based environment to host different applications. It acts as para-virtualization on the standard CPUs and hardware-assisted virtualization on ARM-VE, Intel VT, and NXP QorIQ [103]. The RTOS is specifically certified as SIL 4 according to EN 50128: 2011 [104]. PikeOS datasheet is presented in Table B9 of Appendix B.7.

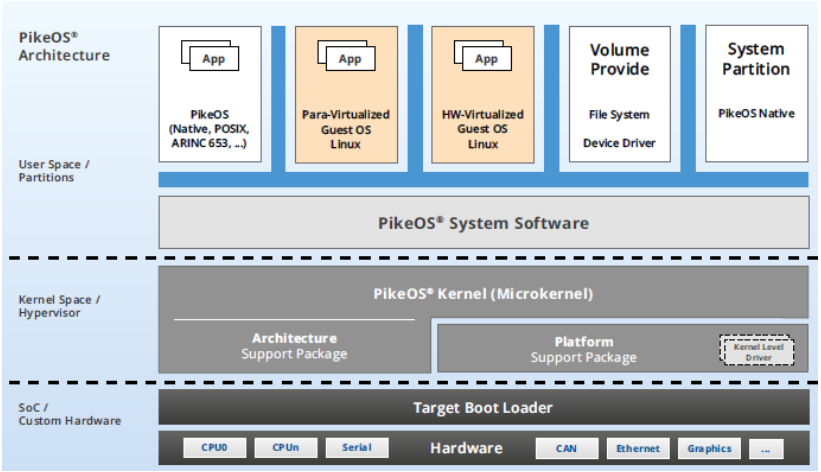

Figure 23: PikeOS hypervisor [103].

PikeOS is integrated with an Eclipse-based IDE CODEO which contains con-

figuration tools, remote debugging (down to the hardware instruction level), target monitoring, remote application deployment, timing analyses, etc. CODEO utilizes GCC compiler and a proprietary debugger. This IDE uses a QEMU based hardware simulation, Simulation Targets, to test and debug applications without requiring any real hardware targets. CODEO can host both Windows and Linux distributions [105]. PikeOS has been used for a SIL 4 CBTC system implemented by SAMSUNG SDS (South Korea), with UDP based communication between the on-board and trackside systems. In that application, PikeOS Hypervisor was implemented on top of a MEN target hardware platform, and existing applications were ported [106].

7 Alternative Development Environment Platforms

After reviewing through different hardware and OS platforms, the thesis will focus now on the last block of the alternative platform, the IDE. It is a software that enables users to develop applications and normally consists of an editor, a compiler and/or interpreter, build automation tools, and a debugger. The developer writes source code in the editor with the compatible programming language/s. The compiler checks the source code, halts the process if the source code does not comply with the language rules, and finally outputs a machine language file. The linker links this file with other library files, checks cross-dependencies and generates an executable file. The debugger runs this file in a controlled manner to monitor the usages of system resources. In the vast majority of the automation industries, IEC 61131-3 compliant languages are used. It is the third part of a ten-part open international standard IEC 61131 developed for a common PLC architecture framework to ease the demands of a software life-cycle. The standard includes the following languages [107]:

Ladder diagram (LD): It is the oldest of the other languages. LD was developed to replace hardwired relay-based control systems. It is also the most widely used, as the developer or the maintenance personnel requires only an electrical background to start programming or begin troubleshooting. The easy visualization of LD is challenged when different functions, e.g. PID loops, trigonometry, data analysis, etc. are required to program. Also, for a larger program, the long-running LD rungs makes program reading cumbersome.

Function Block Diagram (FBD): It provides a better visual understanding for a viewer who is not accustomed with relay logic. The programming blocks are wired as per the operational sequence. But for a large program, FBD can take up a lot of screen space which can make program reading difficult. To write in FBD, the developer needs to put in more efforts to understand the program sequences as it is harder to make changes afterword.

Sequential Function Charts (SFC): It is similar to flowcharts as the starting step is followed by transitions and further steps. SFC is visually most helpful for maintenance engineers to track the progress of a process. But SFC requires extensive planning than other languages, resulting in longer execution times.

Structured Text (ST): It is a high-level language which is faster than the first three graphical languages. The setup is similar as Basic or C. The main difference is that a traditional program does not reach the end until it has finished executing everything, but an ST code runs from start to end many times in a second. ST addresses the complex PLC programming with loops, pointers, easy mathematical function implementations, etc. ST codes can be encapsulated inside the other languages, which is an advantageous feature.

Instruction List (IL): It is a low-level programming language where every line of code executes one operation. This step-by-step approach makes usages of

mathematical functions easier. IL takes less space and enables faster execution but it is not much preferred in the industries due to lack of graphical representations.

IEC 61131 has been criticized for not responding to the needs of the complex decentralized industrial automation systems in terms of reusability, portability, configurability, and interoperability. To address this issue, a component-based, open reference architecture has been developed based on the existing PLC and DCS function blocks. The standard, IEC 61499, replaces the cyclic IEC 61131 model and presents an event-driven function block model where applications can be distributed over multiple resources and devices. A range of IDEs, such as FBDK, ISaGRAF, nxtStudio, etc. support developing applications in IEC 61499 [108].

The IDEs packaged with different OS are discussed in Chapter 6. In the following texts, the proposed third-party IDEs from Chapter 4 will be briefly introduced.

7.1 SCADE Suite

SCADE was developed and owned by Esterel Technologies (France), until in 2012 Ansys, Inc. (USA) had acquired it. Over the years SCADE Suite has been used in designing rail applications, e.g. interlocking, ATO, CBTC, emergency braking systems, over-speed protection, train vacancy detection, etc. [109]. SCADE (Safety Critical Application Development Environment) is a synchronous high-level language to develop safety-critical embedded applications. The foundation of the synchronous language was laid down by three academic languages namely as SIGNAL, ESTEREL, and LUSTRE. These languages were used for real-time control applications to devise a modular system specification, along with simulation, testing, verification and finally producing an embedded executable code. The essential features of these languages prompted different premier organizations and academic institutions to launch the SCADE project, mainly based on LUSTRE. The project has become enriched by added features, such as graphical editors; qualified code generators complying with highest levels of safety standards in avionics, automotive, transportation and nuclear energy applications; mixing of the dataflow type of constructs from LUSTRE with control flow style programming of ESTEREL and SyncChart, etc. [110]. SCADE follows Kahn Process Network theory where different nodes (processes) produce tokens (data elements) which are transferred over a communication channel to the destination nodes. The time between the reception of input and execution of output must be smaller than occurring of the next input. This implies that the internal processing time is almost null, ensuring there is no data overlapping and making the whole process deterministic as the outputs are only determined by the inputs and their occurrences [111].

A typical SCADE model consists of control flow constructs, such as hierarchical state machines comprising of a finite number of states and transitions, and data flow constructs. A corresponding transition condition must be fulfilled for a state to move from its current state to the next state. Only one transition can be fired at a specific time instance. As the computation order is based on functional dependencies,

parallelism is established at the model level. A SCADE model consists of "Operator"s or building blocks, equivalent to a function or procedure in any other languages. In the suite, there are some basic pre-defined blocks available, e.g. mathematical, comparison, logical, array, time, choice, bitwise, and higher-order. These basic blocks are used to make higher-level operators. SCADE is also featured with a set of libraries to immediately start designing models [112].

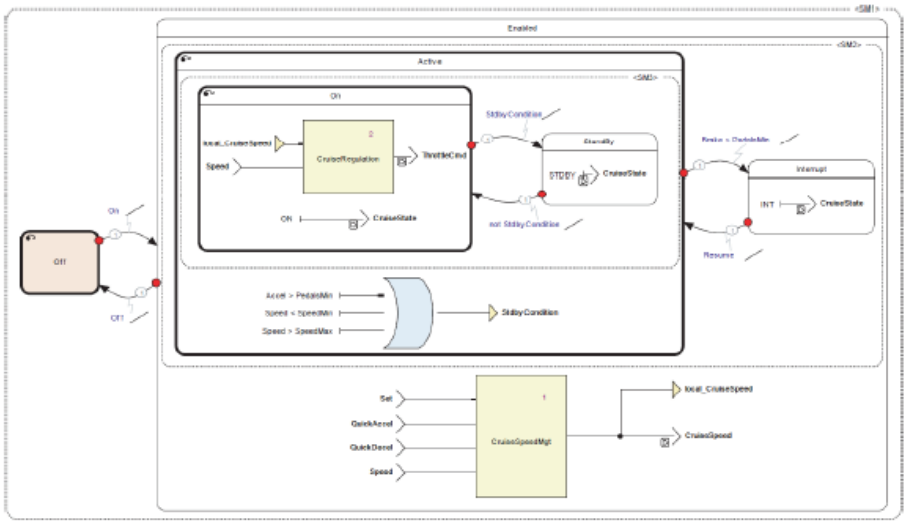

Figure 24: SCADE interface [112].

A function called "Checker" checks for any syntactical or semantic mistakes in the prepared project. If it is error-free then a machine-readable, traceable, optimized, target-independent, and customizable C or Ada code is generated via the proprietary compiler, KCG. The code is deterministic as the output model always produces the same generated code with the same KCG parameters. The compiler is certified to SIL 3 as per IEC 61508:2010 and SIL3/4 as per EN 50128:2011 [76]. The generated code is modular in terms of static memory allocation and finite execution duration. Also, there are customizable RTOS adaptors available for the generated code. KCG is packed with a dedicated Python-based API, which initiates and runs the model. Through this API, generated code can be customized for renaming the objects and top-level interfaces. In the SCADE suite, there are options for installing dedicated code generators, e.g. wrappers. SCADE Suite is equipped with code analysis tools, such as Timing and Stack Optimizer which verifies the timing requirements of the KCG code for a specific processor target by estimating the worst-case execution time, and monitors stack usage by an application; Design Verifier to find bugs in the early development process; and C Compiler Verification Kit which contains C constructs and their combinations up to a certain level of complexity that can be generated by the compiler. SCADE has been used by CASCO (China) to develop a CBTC system (iCMTC) for Shanghai Metro [113]. There are no other project details available in the public domain. The datasheet of SCADE is presented in Table B10 of Appendix B.8.

7.2 FlexiSafe

FlexiSafe is developed by infoteam Software AG (Bubenreuth, Germany) which was a leading co-designer for IEC 61131 standard. The company has been active on the market for almost 40 years in the fields of transportation, infrastructure, life sciences, and public services [114]. FlexiSafe is based on ISaGRAF framework which was originally developed by ICS Triplex, now owned by Rockwell Automation. ISaGRAF is scalable and portable to different hardware and operating systems associated with both centralized and distributed architectures. It consists of a workbench and a SoftPLC runtime. The workbench allows for the writing applications in Windows and Linux environments with IEC 61131-3 set of programming languages along with the relatively newly proposed IEC 61499 function blocks. It also supports functions and function blocks written in IEC 61131-3 and Flow Chart language. The application is compiled by the runtime to produce target-independent code (TIC) or target-specific C source code [115].

FlexiSafe has adopted the basic ISaGRAF framework and added additional features, e.g. a "diverse" compiler which generates language-neutral XML graphs to check for the compiler output considering structure, flow, variables, and parameters. The IDE has been used in 850,000 runtimes, spanning over 14 years in different safety-critical applications. FlexiSafe kernel contains a TIC engine which is protected by safety wrappers. The developer must ensure that non-safe applications do not interfere with the safe elements inside the kernel. There are a bunch of development and code analysis tools, such as Cause and Effect Editor which enables programmers to generate codes efficiently which simplifies the safety verification process. The IDE is integrated with functions, e.g. "bypass" and "force" which is important in project commissioning. FlexiSafe is also equipped with Dependency Trees, which is a list of variables derived from or contributing to the root. It is important for SIL verification. Dependency Tree is used by a static analyzer that acts on the source or object code while they are executing. Version control and cross-reference browser are also packed in the FlexiSafe environment [116]. FlexiSafe runtime engine along with the PLCopen function blocks complies as per SC3 according to IEC 61508: 2010 and SIL 4 according to EN 50128: 2011 [117]. The safety certification is displayed in Figure A13 in Appendix A.6.

A safety-critical system, iFSC is proposed by infoteam including F75P target hardware from MEN Mikro, QNX Neutrino RTOS Safe Kernel (QOS), and FlexiSafe programming environment [118]. It is certified up to SIL 3 as per IEC 61508:2010 [76]. FlexiSafe/ISaGRAF has been in use for mostly on-board applications in different railway systems worldwide. EKE Electronics (Finland) uses ISaGRAF in its EKE-Trainnet to integrate all the on-board systems via TCN. It controls and monitors sub-systems, such as doors, lights, HVAC, brakes and batteries, passenger information system (PIS), etc. CAF (Spain) uses an ATP system from SEPSA (Spain) which is based on ISaGRAF. Bombardier and Alstom have used ISaGRAF in multiple applications to control subsystems, such as traction, braking, speed limit, air conditioning, etc. SP Teknik (Denmark), in cooperation with NAUTSILUS (Russia), has developed a PIS based on Linux, where ISaGRAF applications can be ported.

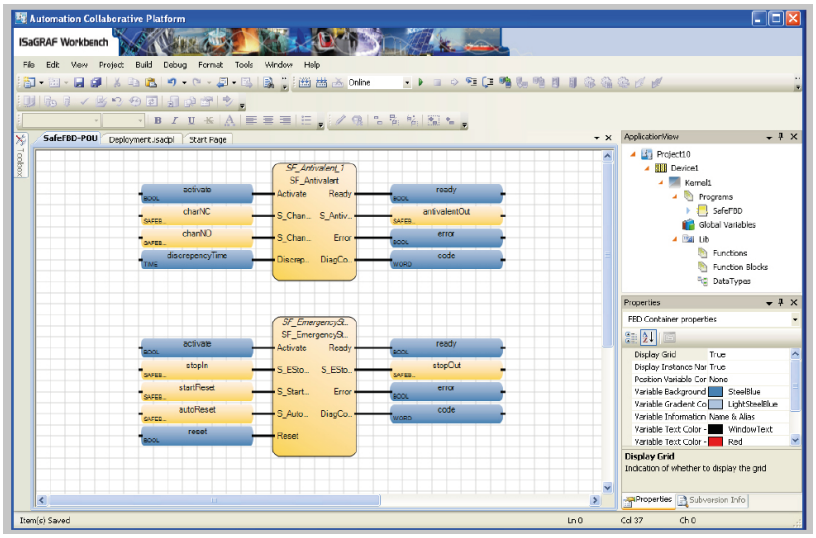

Figure 25: FlexiSafe environment [116].

The other use cases involve PIS from Kontron (Belgium), traction control in Alstom's TestStand controller, on-board control system in Alspa CX90 from Soprano Industry (France), door control in Virgin Trains (UK), Prague Metro's diagnostic platform by UniControls (Czech Republic), etc. [119]. The datasheet of FlexiSafe is presented in Table B11 of Appendix B.9.

7.3 Prover Trident

It is offered by Prover Technology AB (Stockholm, Sweden) which is a company focussing on formal methods and software development for safety-critical systems [120]. The company aims at reducing the duration of railway interlocking project developments by 50%, with the introduction of the Prover Trident suite which consists of the following elements [121]:

PiSPEC IP: It is a predicate logic-based formal language which models signalling requirements in a clear way to avoid discrepancies in writing the specifications by hand. PiSPEC IP has a strict type system and object orientation covering classes, inheritances, and interfaces. The generated formal requirements can be stored in a library for future reuse.

Prover iLock: This is an IDE which translates the generic applications formalized by PiSPEC IP to a specific application by graphical configuration and automatic source code generation. In the editor, rail tracks are drawn and trackside elements are placed from the libraries in a drag-and-drop manner. It consists of other features, such as iLock Verifier to formally verify whether the generated code has satisfied the system requirements; iLock Simulator to debug and perform functional testing of all the test cases; and iLock Documenter for generating control tables and test/verification reports.

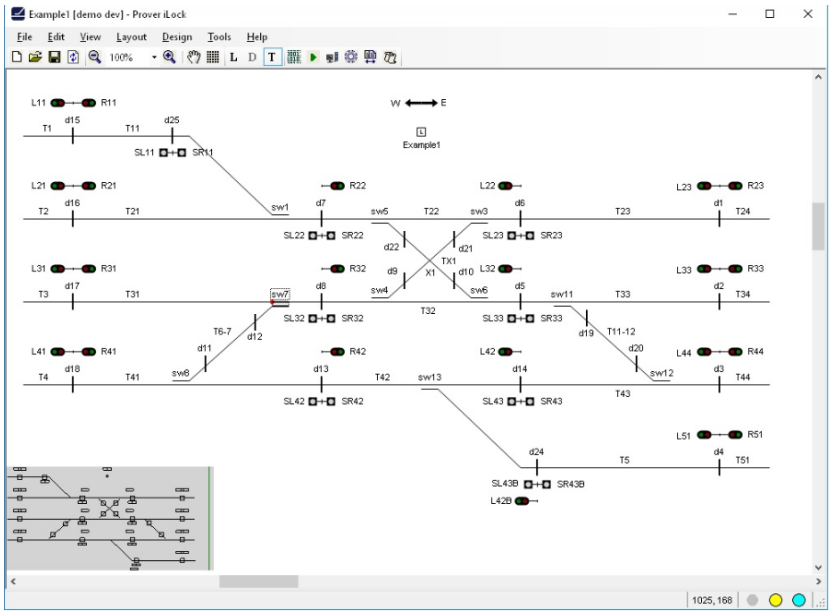

Figure 26: Prover iLock [122].

Prover Certifier: It is an EN 50128 SIL 4 certified sign-off verification tool which generates safety evidence. This tool minimizes human dependency by eliminating the need for code reviews and safety testing.

The Prover Trident package or parts of it are in use for several railway applications. The New York City Transit uses Prover iLock Verifier for formal verification of the interlocking software which is based on Westrace Mk II (Siemens), MELLOCK (Mitsubishi), iVPI (Alstom), and Microlok II (Ansaldo STS). Canadian Pacific implements the complete Prover iLock package to develop applications for the interlocking system built with ElectroLogIXS (General Electric) and Microlok II (Ansaldo STS). Stockholm Metro (Sweden) and Network Rail (UK) have used the complete Prover iLock suite for developing the interlocking system based on target hardware platforms from General Electric and Siemens, respectively. Paris Metro (RATP, France), Bane NOR (Norway) and Infrabel (Belgium) uses Prover Certifier, iLock Verifier and PiSPEC, respectively [123]. The datasheet of Prover Trident is presented in Table B12 of Appendix B.10.

7.4 CODESYS Safety

CODESYS is one of the leading IEC 61131-3 automation software, produced by 3S-Smart Software Solutions (Kempten, Germany). It has been used in over 2 million applications in different industries. This IDE can be applied on CODESYS compatible target hardware platforms. CODESYS Safety comes as an add-on package for the standard IDE, CODESYS Development System. The safety controller appears as a sub-node of the standard controller with specific application, tasks, I/O in the editor layout. Different safety controllers communicate via Safety NetVars. The developer

can program the safe functions via FBD safety editor and non-safe functions are designed with IEC 61131-3 set of languages. The IDE includes additional safety functions, such as safe versioning, change tracking, safe debug mode, etc. The runtime toolkit package includes, runtime system components, system configurator, adaptive interfaces, and manuals. CODESYS Test Manager produces automated test cases, instructions, and reports. The IDE supports target platforms from TriCore, ARM, and PowerPC [124].

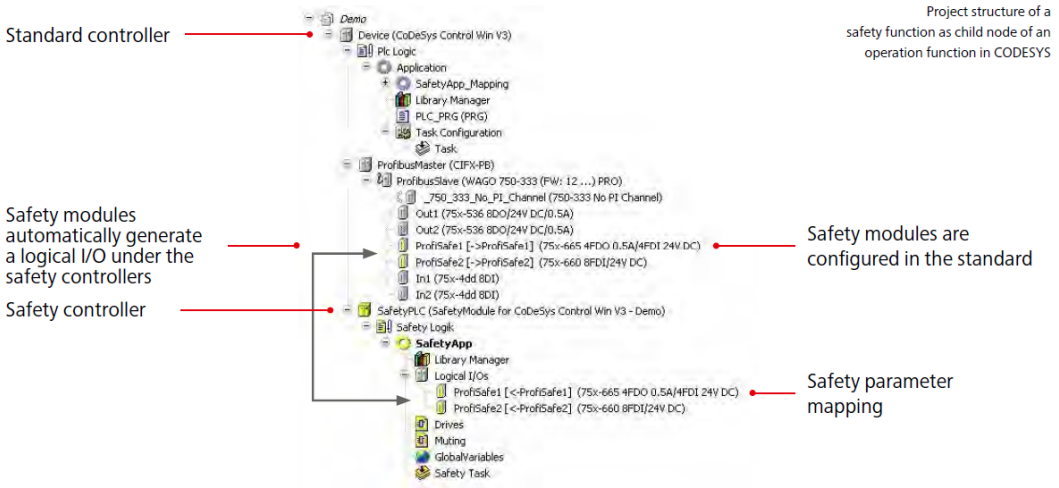

Figure 27: CODESYS Safety environment [124].

The runtime system and PLCopen function blocks with associated libraries and fieldbus configuration are certified to SIL 3 according to IEC 61508: 2010. The programming system compiler complies with the tool class T3 requirements as per IEC 61508-3 [125]. The safety certification is displayed in Figure A14 in Appendix A.7. The safety package includes, certification reports, test framework, automated test scripts for verification of the runtime system, and the compiler. CODESYS Safety has been in use for applications from Bosch Rexroth AG, Berghof Automationstechnik GmbH, Yacoub Automation GmbH, KEB GmbH and Kendrion Kuhnke Automation GmbH [124]. The datasheet is presented in Table B13 of Appendix B.11.

8 Final Cost-based Analysis

Based on the thesis methodology prescribed in Chapter 4 and the different alternative hardware, OS, and IDEs described in Chapter 5, Chapter 6 and Chapter 7 respectively, a comparative analysis is presented in the following texts. This discourse refers to the respective datasheets in the appendices. Information regarding prices is not considered, as per the non-disclosure agreements with different vendors.

8.1 Hardware: Cost-based Analysis

This section compares the alternative hardware platforms, CSP and MH50C, based on the datasheets presented in Table B4 in Appendix B.2, and Table B5 in Appendix B.3, respectively. The comparative parameters are as follows:

CPU Architecture

The modern CPU architecture comes in multi-core, multi-threaded offerings. The benefits of threads can only be capitalized by writing suitable applications. For example, in case of an application that mostly does calculations, one thread per core is a reasonable decision. This is because more threads might result in an overhead. But in case of I/O operations, higher number of threads are required to run parallel processes to cater to all the requests within a specified time limit. If the interlocking applications are developed to leverage the advantages of parallel programming, the number of threads could be a vital factor. The NXP QorIQ P1/P2 processors used in the CSP are of PowerPC e500 architecture. The processors in the Master and Checker CPUs are of the dual-core single-thread type and the I/O processor is of the single-core single-thread architecture. The MH50C uses three Intel Atom E680T processors which are based on single-core dual-thread type Tunnel Creek (Queens Bay Platform) architecture. These multiple threads enable thread-level parallelism which in turn improves memory miss latency. Also, the processors support Intel VT-x, meaning any RTOS capable with virtualization capabilities can be easily integrated with the MH50C platform.

Clock Frequency

Although CPU clock frequency is an important parameter mostly when it comes to comparing between processors from the same family of architectures, it is still considered here for the sake of the argument. The comparison can only be established by running same programs on both the platforms and calculating the respective cycle times. The CSP processors are clocked in the range of 800-1200 MHz while the processors in the MH50C offer a frequency of 1600 MHz.

CPU Synchronization

For a safety-critical hardware platform, synchronization between redundant CPUs is an important factor. SMART EC offers a unique data lockstep mode which establishes

determinism for modern CPU architectures. It provides both hardware (SRB) and software (DCA) arrangements to synchronize the CSP CPUs. Despite following the old hard lockstep technique, the MH50C provides software based EN 50128: 2011 (SIL 4) and IEC 61508: 2010 (SIL 3) certified proprietary function SyncLayer to synchronize two CPs in F75P. This eliminates the hardware maintenance efforts during the platform's life-cycle.

Memory

Although the L2 and L1 instruction cache memory associated with both the platforms are same (512 KB and 32 KB, respectively), the L1 data cache in the CSP (32 KB) is bigger than that of in the MH50C (24 KB). Therefore, it is easier to fetch frequently used data to be used in CPU operations for the CSP platform. The maximum RAM that can be attached with the MH50C platform is 2 GB (DDR2), whereas the CSP can accommodate a maximum of 4 GB RAM (DDR3). DDR3 type of memory has some obvious advantages over DDR2 in terms of higher bandwidth and optimized power consumption. The cache and the main memory of the CSP processors are equipped with error-correcting code (ECC) mechanism, which can detect and correct data corruption. The MH50C does not offer any ECC support.

I/O

In railways, mostly digital I/O are used along with counter modules for axle counters. I/O capacity is an important factor for choosing a particular hardware platform. SMART EC provides a single module (cIOU-DIO) to accommodate both digital inputs and outputs. The output channels can be also be used for frequency counting. Up to 48 I/O channels can be accommodated in each CSP platform. The I/O capacity can be increased by integrating the Expansion Box Platform via safe communication protocols. MEN Mikro offers separate modules for both inputs (K2) and outputs (K1 and K7). There is no counter module available as of now. In one platform, 24 I/O channels can be used at SIL 4. A single MH50C platform is capable to handle up to 1500 DI and 600 DO.

Communication

In a safety-critical platform, safe communication is established between all the control hardware as per EN 50159. Traditionally, vendors supply the PLC package with their proprietary communication protocols. SMART EC has not publicly disclosed any information regarding their protocol. There are separate communication modules for third-party data transfers via MVB, CAN and UART. MEN Mikro uses EN 50159 certified FSoE protocol to guarantee deterministic data transfer with a failure rate of 10^{-9} packets per hour and maximum response time of 5 ms. The proprietary PACY framework acts on top of the FSoE. There are provisions of external communications via MVB, CAN, and Profinet.

Operating Temperature

To be globally acceptable, a hardware platform must be tolerant enough to be installed in various climatic situations. A wider temperature range helps to reduce costs and efforts related to cooling and/or heating arrangements. Both the alternative platforms can operate in temperatures as low as –40°C, which is a significant improvement from the present HIMA platform. For the CSP, the upper threshold for operating temperature in the open rack condition is +60°C. With integrated fan trays, the platform can work efficiently up to +70°C. The MH50C is capable to operate at +70°C in the open condition and +85°C with forced cooling arrangements.

Certification

It is one of the deciding factors in choosing the alternative platforms, as described in Chapter 4. The hardware platforms must conform to the highest levels of safety as per IEC 61508 and EN 5012x. SMART EC underwent for certification of the CSP along with VxWorks 653 RTOS. There is no unique certification for the hardware platform itself, meaning that the customers would have to go through a strenuous certification effort if choosing for a different RTOS. MEN Mikro provides separate SIL certifications for both the standalone CPU module (F75P) and the whole package along with the QOS BSP. This signifies that if the customer opts for an RTOS other than QOS, there will be minimal certification efforts involved.

Planned Product Life

Depending on the frequently changing market, vendors update their electronic components with newer versions for better speed, memory chip density, storage device capacity, data transmission rate, etc. This could cause product obsolescence for the customer in the near future. The suppliers must commit to their customers with a planned product life, guaranteeing that in case of failures, the affected product would be replaced with the same versions. SMART EC promises a product life of 15 years for the CSP, whereas the MH50C has a life-span of 10 years.

Brand Value

SMART EC has provided documented use cases where the CSP and other platforms are used as illustrated in Chapter 5.1. In most of these applications legacy systems are upgraded and either the old I/O modules are kept or new customized ones are provided. In case of the MH50C, although it has been in use for wayside, rolling stock, and ERTMS applications, there are no publications available in the public domain.

Cost Assignment

Table 4: Comparative analysis of alternative hardware platforms.

Parameter	Weight	CSP		MH50C	
		Score	Cost	Score	Cost
CPU Architecture	1	4	4	5	5
CPU Frequency	0.5	4	2	5	2.5
CPU Synchronization	0.5	4	2	5	2.5
Memory	0.5	5	2.5	4	2
I/O	1	5	5	4	4
Communication	1	4	4	5	5
Operating Temperature	0.5	4	2	5	2.5
Certification	1	4	4	5	5
Planned Product Life	1	5	5	4	4
Brand Value	1	5	5	4	4
Standalone Hardware Cost		$C(H_1)$ =35.5		$C(H_2)$ =36.5	

8.2 Operating Systems: Cost-based Analysis

This section compares the alternative OS platforms, VxWorks 7, QOS, INTEGRITY, and PikeOS, based on the datasheets presented in the Table B6 in Appendix B.4, Table B7 in Appendix B.5, Table B8 in Appendix B.6, and Table B9 in Appendix B.7, respectively. The comparative parameters are as follows:

Scheduling Policy

An OS is equipped with scheduling algorithms to decide about which processes are going to be served, while keeping in mind various criteria, such as CPU utilization, throughput, wait time, response time, etc. Both VxWorks 7 and QOS are equipped with the popular priority-based preemptive schedulers. Also, there is a provision to use other schedulers, such as round-robin, adaptive scheduling, etc. as per the requirements. INTEGRITY and PikeOS offer only the priority-based preemption scheme to schedule the processes.

AMP/BMP/SMP Support

In modern hardware architecture, several CPUs share the same resources. Depending on whether all the CPUs execute the same piece of program/process/thread there are different multiprocessing techniques. In asymmetric multiprocessing (AMP) multiple OS use their own specific CPUs, whereas in symmetric multiprocessing (SMP) a single OS can use multiple CPUs simultaneously. The bound multiprocessing (BMP) is similar to SMP, but the user has the control to select the processor on which a

particular thread would run. BMP has some distinct advantages, e.g. elimination of the possibility of cache thrashing, simpler debugging, easier migration of legacy software, etc. A particular RTOS must be equipped with all the three techniques giving the user a wide range of options to optimize resources. Both VxWorks 7 and QOS are equipped with AMP, BMP and SMP techniques, whereas for INTEGRITY and PikeOS there is no BMP support.

Networking

This feature allows an RTOS to interface with other systems. If there are more networking protocols available, then a platform is more flexible to integrate with different kind of systems. Apart from the traditional TCP/IP, VxWorks 7 is packed with the new "buzz" time-sensitive networking (TSN) which enables hierarchical automation pyramid elements of different bandwidths to connect with each other. TSN guarantees that higher-level protocol layers can share a common network architecture, and latency times of real-time critical data can be guaranteed throughout the network. The other three alternative RTOS platforms have only the TCP/IP capabilities to offer.

Connectivity

An OS must support different kinds of interface standards to connect with different devices for seamless real-time data transfer. Generally, universal serial bus (USB) is the typical industrial standard along with IEEE 1394 (high-performance serial bus). An alternative OS platform must also be equipped with the newer standards, as offered by the telecommunications industry, for secure and faster data transfer. VxWorks 7 offers OPC-UA and CAN possibilities whereas QNX and INTEGRITY provide Wi-Fi, Bluetooth and NFC capabilities. PikeOS is packed with USB capabilities only.

Certification

It is very critical that the alternative OS platform must meet manufacturer design process requirements of corresponding SIL values to achieve sufficient integrity against systematic errors of design. Apart from the generic safety standard IEC 61508, the RTOS must also comply with the railway specific EN 50128 to save certification efforts from the customer's end. Both VxWorks and QOS provide SIL 3 capabilities as per IEC 61508 when used as individual products. Also, both of the respective vendors have collaborated with SMART EC and MEN Mikro to produce SIL 4 certification according to EN 50128. The downside is, if VxWorks and QNX are used on other alternative hardware platforms, then the certification efforts will be time-consuming and costly. But for INTEGRITY and PikeOS, there are separate IEC 61508 (SIL 3) and EN 50128 (SIL 4) certifications available.

Brand Value

A particular OS is also judged by its lifetime in the industry, collaboration with different rail vendors, and future roadmap for the newer versions to avoid obsolescence. Both Wind River and QNX/Blackberry are in the OS market for more than three decades, experiencing through the changing industrial needs. They have a strong portfolio of rail integrators. Both these vendors have a high reputation when it comes to a new API for a third-party vendor or delivering a new BSP for a new hardware platform. Green Hills Software is a dominant force in the defence industries in the USA, delivering generations of INTEGRITY products satisfying stringent safety requirements. INTEGRITY is now being adopted into rail applications too. SYSGO is a rail-focused RTOS vendor, but their portfolio is not stronger than Wind River and QNX/Blackberry.

All the RTOS are bundled with their respective IDEs as described in Chapter 6. This gives the customers an option to start developing the applications right away, without requiring any other third-party platforms.

Programming Language

All these IDEs are based on high-level programming languages to cater to a broad range of customers with different needs. Apart from the traditional C and C++ languages, Workbench, Momentics and MULTI IDE offer support for Python, Ada, and Rust etc. The PikeOS IDE, CODEO, can accommodate only C and C++.

Host OS Support

The IDE should be flexible enough to be hosted on a range of general-purpose OS. Workbench, MULTI IDE and CODEO can be hosted on different versions of Windows and Linux, whereas Momentics is compatible with macOS also.

Target OS Support

The IDE compilers should be able to produce a code that can be ported to any other OS. Other than the respective legacy RTOS platforms, applications from Workbench, MULTI IDE and CODEO can be ported to Windows, Linux, OSE, ThreadX, etc. Codes written MULTI IDE can even be ported to VxWorks 7. But Momentics can port applications only to the legacy QNX OS.

Certification

The IDE toolchains should fulfil the requirements for T3 tools as per IEC 61508 and EN 50128. MULTI IDE has the required certifications for both the standards, while the others have been certified as per IEC 61508 only.

Cost Assignment

Table 5: Comparative analysis of alternative OS platforms.

Parameter	Weight	VxWorks7		QOS		INTEGRITY		PikeOS	
		Score	Cost	Score	Cost	Score	Cost	Score	Cost
Scheduling Policy	1	5	5	5	5	3	3	4	4
AMP/BMP/SMP Support	1	5	5	5	5	3	3	3	3
Networking	0.5	5	2.5	4	2	4	2	4	2
Connectivity	0.5	5	2.5	5	2.5	5	2.5	3	1.5
Certification	1	4	4	4	4	5	5	5	5
Brand Value	1	5	5	5	5	4	4	4	4
IDE Properties									
Parameter	Weight	Workbench		Momentics		MULTI IDE		CODEO	
		Score	Cost	Score	Cost	Score	Cost	Score	Cost
Languages	1	5	5	5	5	5	5	4	4
Host OS Support	0.5	4	2	5	2.5	4	2	4	2
Target OS Support	0.5	5	2.5	4	2	5	2.5	5	2.5
Certification	1	4	4	4	4	5	5	4	4
Standalone OS Cost		$C(O_1)$=37.5		$C(O_2)$=37		$C(O_3)$=34		$C(O_4)$=32	

8.3 Development Environment: Cost-based Analysis

This section compares the alternative IDE platforms, SCADE, FlexiSafe, Prover Trident, and CODESYS Safety, based on the datasheets presented in Table B10 in Appendix B.8, Table B11 in Appendix B.9, Table B12 in Appendix B.10, and Table B13 in Appendix B.11, respectively. The comparative parameters are as follows:

Framework

It is the foundation which allows the developer to access a specific set of tools to write programs. The proposed IDE should preferably be equipped with similar features of the present SILworX platform to ease the development efforts. FlexiSafe and CODESYS Safety offer similar IDE layout as of the present platform with the availability of IEC 61131-3 compliant language tools. Furthermore, FlexiSafe offers integration of IEC 61499 function blocks and C language. Prover Trident is a unique IDE where informal system requirements are first transformed into formal design principles, and then applications are developed by drawing tracks and linking subsequent library elements. The learning curve for this IDE is steeper than that of the others. But once the formal requirements are ready, applications can be written in a short time. In SCADE, model-based programming is employed with hierarchical state machines and data flows. The modular programming offers the highest flexibility to change the application parts with minimal efforts. But the problem with this type of programming is to find the stable states for a large interlocking application. If not

properly planned, it is quite possible to drive the system into deadlocks. Without any prior knowledge of finite state machines, developing applications in SCADE is quite complicated.

Development Tools

These are very important gadgets for efficient programming. SCADE, FlexiSafe and CODESYS Safety contain the basic tools for software development, such as editor, compilers, debuggers, linkers, version controllers, etc. Apart with that there are tools for static analyses, APIs to include third party software, extensive ready-to-use libraries to start developing programs instantly, verification and validation tools for design and written code, etc. In addition to these features, Prover Trident is equipped with Prover Certifier which is the only sign-off tool present in the railway sector. It verifies the application and produces safety evidence according to EN 50128 (SIL 4). This significantly reduces time and cost spent on running test cases and doing code reviews. As mentioned in Chapter 7.3, a lot of customers have only used this certification tool from the Trident package, to verify their own codes.

Certification

To develop a safety-critical application, the run time engine, workbench, and the associated libraries offered by the IDE must be certified to the highest levels of safety as per the generic and rail-specific standards to ensure that a safe code is ported to the target system. SCADE, FlexiSafe and Prover Trident are certified to SIL3 as per IEC 61508:2010 and EN 50128:2011, while CODESYS Safety is only certified as per the generic standard. This might make the rail application developers sceptical about using CODESYS Safety.

Application

The brand value and examples of use cases make a certain IDE platform more acceptable to the user. As software updates are very frequent, there should be a roadmap available for the customers to check for the backward compatibility. Out of all the IDEs, SCADE has the best reputation and great collaborations with different railway vendors. If not for writing the main applications, different elements from SCADE suite have been used for various parts of a project management. But most of these examples are not available in the public domain. Due to the legacy of ISaGRAF, FlexiSafe has an extensive range of applications around the world for both on-board and wayside cases as presented in Chapter 7.2. Prover Trident has also been used for both wayside and on-board projects. Mainly, the verification toolkit Prover Certifier was customers' choice to check if the written code is SIL 4 capable. Being a new technology in the respectively rigid railway market, Prover Trident is taking some time to gain confidence. Although the generic CODESYS platform is quite popular in manufacturing automation for the past two decades, the absence of rail-specific certification and being a target-specific platform makes it the least suitable choice for an alternative IDE platform.

Cost Assignment

Table 6: Comparative analysis of alternative IDE platforms.

Parameter	Weight	SCADE		FlexiSafe		Prover Trident		CODESYS Safety	
		Score	Cost	Score	Cost	Score	Cost	Score	Cost
Framework	1	3	3	5	5	4	4	5	5
Development Tools	0.5	4	2	4	2	5	2.5	4	2
Certification	1	5	5	5	5	5	5	3	3
Application	1	4	4	5	5	4	4	3	3
Standalone IDE Cost		$C(O_1)$=14		$C(O_2)$=17		$C(O_3)$=15.5		$C(O_4)$=13	

8.4 Compatibility: Cost-based Analysis

The comparative parameters are as follows:

BSP Availability

It is a program which acts as the interface between the RTOS and the processor, memory, and system buses of the target hardware platform. Typically it is linked with a set of libraries to provide support for interrupt generation and handling, memory mapping, and clock synchronization. The BSP enables the RTOS kernel to utilize the hardware resources. The chosen alternative OS platform should be able to supply a BSP suiting the target hardware architecture. Wind River provides VxWorks 7 BSP for architectures used in both the CSP and MH 50C platforms. Moreover, SMART EC and Wind River have a collaborative railway specific safety certification together. Similarly, a QOS BSP is available to work on the MH50C. For the CSP, Blackberry offers the generic QNX Neutrino BSP. Since QOS is based on Neutrino, a specific BSP for CSP can be easily developed. Although there are no certification efforts from SYSGO GmbH with the chosen alternative hardware platforms, it offers BSPs for the corresponding architecture families. This means that there are no exclusive, tried and tested BSPs available. Kontron's upcoming SAFe-VX hardware is under the combined certification process with PikeOS, which makes it a probable future option to be used as an alternative platform [126]. Like SYSGO, Green Hills Software provides BSPs for the all the popular architectures, but without any collaborative efforts with hardware vendors discussed in this thesis.

Collaborative Certification Efforts

As stated earlier, there are collaborations between SMART EC and Wind River, and MEN Mikro and QNX/Blackberry. These are also taken into account in the comparison.

Code Portability

It is a parameter of the highest priority as the compiled source code must run on the chosen OS platform. The compiled C or Ada codes from FlexiSafe and Prover Trident can be ported to any safe RTOS. This gives the system integrator a wide range of options to choose from different RTOS based on the project requirements. Barring QNX, the generated code from SCADE's KCG can be ported to other alternative RTOS discussed in the thesis. ANSYS provides customizable adaptors to adapt to other RTOS. CODESYS Safety codes can only be ported to VxWorks 7 and QOS.

Cost Assignment

Table 7: Comparative analysis of compatibility factors between alternative platforms.

Hardware Platform	Weight	VxWorks7		QOS		INTEGRITY		PikeOS	
		Score	Cost	Score	Cost	Score	Cost	Score	Cost
Parameter: BSP Availability									
CSP	1	5	5	5	5	3	3	3	3
MH50C	1	5	5	5	5	3	3	3	3
Parameter: Collaborative Certification Effort									
CSP	1	5	5	3	3	3	3	3	3
MH50C	1	3	3	5	5	3	3	3	3
OS Platform	Weight	SCADE		FlexiSafe		Prover Trident		CODESYS Safety	
		Score	Cost	Score	Cost	Score	Cost	Score	Cost
Parameter: Code Portability									
All	1	4	4	5	5	5	5	3	3
Simplified Table									
Hardware Platform		VxWorks7		QOS		INTEGRITY		PikeOS	
CSP		$C(H_1, O_1)$=10		$C(H_1, O_2)$=8		$C(H_1, O_3)$=6		$C(H_1, O_4)$=6	
MH50C		$C(H_2, O_1)$=8		$C(H_2, O_2)$=10		$C(H_2, O_3)$=6		$C(H_2, O_4)$=6	
OS Platform		SCADE		FlexiSafe		Prover Trident		CODESYS Safety	
All		$C(O_k, E_1)$=4		$C(O_k, E_2)$=5		$C(O_k, E_3)$=5		$C(O_k, E_4)$=3	

8.5 Final Cost-based Analysis

In this section, the final costs of all the possible 32 combinations are presented. For example, the cost of an alternative platform containing CSP, VxWorks 7 and SCADE as hardware, OS and IDE respectively is calculated as follows:

$$\begin{aligned} C(H_1, O_1, E_1) &= C(H_1) + C(O_1) + C(E_1) + C(H_1, O_1) + C(O_1, E_1) \\ &= 35.5 + 37.5 + 14 + 5 + 5 + 4 \\ &= 101 \end{aligned}$$

Similarly, all the other costs are calculated as represented in the Table 8.

Table 8: Final costs of the possible combinations.

Combination	Cost	
CSP + VxWorks 7 + SCADE	$C_1(H_1, O_1, E_1)$	101
CSP + VxWorks 7 + FlexiSafe	$C_2(H_1, O_1, E_2)$	105
CSP + VxWorks 7 + Prover Trident	$C_3(H_1, O_1, E_3)$	103.5
CSP + VxWorks 7 + CODESYS Safety	$C_4(H_1, O_1, E_4)$	99
CSP + QOS + SCADE	$C_5(H_1, O_2, E_1)$	98.5
CSP + QOS + FlexiSafe	$C_6(H_1, O_2, E_2)$	102.5
CSP + QOS + Prover Trident	$C_7(H_1, O_2, E_3)$	101
CSP + QOS + CODESYS Safety	$C_8(H_1, O_2, E_4)$	96.5
CSP + INTEGRITY + SCADE	$C_9(H_1, O_3, E_1)$	93.5
CSP + INTEGRITY + FlexiSafe	$C_{10}(H_1, O_3, E_2)$	97.5
CSP + INTEGRITY + Prover Trident	$C_{11}(H_1, O_3, E_3)$	96
CSP + INTEGRITY + CODESYS Safety	$C_{12}(H_1, O_3, E_4)$	91.5
CSP + PikeOS + SCADE	$C_{13}(H_1, O_4, E_1)$	91.5
CSP + PikeOS + FlexiSafe	$C_{14}(H_1, O_4, E_2)$	95.5
CSP + PikeOS + Prover Trident	$C_{15}(H_1, O_4, E_3)$	94
CSP + PikeOS + CODESYS Safety	$C_{16}(H_1, O_4, E_4)$	92
MH50C + VxWorks 7 + SCADE	$C_{17}(H_2, O_1, E_1)$	100
MH50C + VxWorks 7 + FlexiSafe	$C_{18}(H_2, O_1, E_2)$	104
MH50C + VxWorks 7 + Prover Trident	$C_{19}(H_2, O_1, E_3)$	102.5
MH50C + VxWorks 7 + CODESYS Safety	$C_{20}(H_2, O_1, E_4)$	98
MH50C + QOS + SCADE	$C_{21}(H_2, O_2, E_1)$	101.5
MH50C + QOS + FlexiSafe	$C_{22}(H_2, O_2, E_2)$	105.5
MH50C + QOS + Prover Trident	$C_{23}(H_2, O_2, E_3)$	104
MH50C + QOS + CODESYS Safety	$C_{24}(H_2, O_2, E_4)$	99.5
MH50C + INTEGRITY + SCADE	$C_{25}(H_2, O_3, E_1)$	94.5
MH50C + INTEGRITY + FlexiSafe	$C_{26}(H_2, O_3, E_2)$	98.5
MH50C + INTEGRITY + Prover Trident	$C_{27}(H_2, O_3, E_3)$	97
MH50C + INTEGRITY + CODESYS Safety	$C_{28}(H_2, O_3, E_4)$	92.5
MH50C + PikeOS + SCADE	$C_{29}(H_2, O_4, E_1)$	92.5
MH50C + PikeOS + FlexiSafe	$C_{30}(H_2, O_4, E_2)$	96.5
MH50C + PikeOS + Prover Trident	$C_{31}(H_2, O_4, E_3)$	95
MH50C + PikeOS + CODESYS Safety	$C_{32}(H_2, O_4, E_4)$	90.5

As per the calculations, the combination $C_{22}(H_2, O_2, E_2)$ has the highest cost of 105.5. This platform is based on MH50C, QOS, and FlexiSafe. The reasons are, the capable hardware architecture of MH50C; the reputation of QNX Neutrino kernel; the collaborative certification between MH50C and QOS BSP; the capability of producing TIC by FlexiSafe along with the IEC 61131-3 friendly environment; and

the proposed iFSC system by infoteam Software AG with extensive applications in the railway sector. $C_2(H_1, O_1, E_2)$ is the close second to the best combination, with a cost of 105 because of similar reasons, e.g. collaborative efforts between SMART EC, and Wind River and the abilities of FlexiSafe. Other combinations, such as $C_{18}(H_2, O_1, E_2)$ and $C_3(H_1, O_1, E_3)$ have costs closer to the highest one due to Wind River's readymade BSP for MH50C and Prover Trident's efficient way of developing interlocking applications, respectively.

The worst combinations are $C_{32}(H_2, O_4, E_4)$ and $C_{12}(H_1, O_3, E_4)$ with costs of 90.5 and 91.5, respectively. This is because of insufficient target specific BSP support from Green Hills Software and SYSGO GmbH; lack of rail-specific safety certification for CODESYS Safety and its inability to port code to the concerned OS platforms; and mediocre brand values of INTEGRITY and PikeOS compared to the other OS alternatives. Similar costs are observed in the combinations $C_{13}(H_1, O_4, E_1)$ and $C_{29}(H_2, O_4, E_1)$ with 91.5 and 92.5, respectively. This is due to the previously mentioned BSP issues and higher learning curve of SCADE environment.

9 Conclusions and Future Work

In this thesis, different COTS and safety-certified components required for building an interlocking system have been investigated. Based on the technical characteristics and interoperability, these components and their combinations have been awarded with costs. To maintain simplicity, the hardware, OS, and IDE platforms are considered as linear systems and the final cost is deduced on the basis of the superposition principle. This can be a point of argumentation as the mathematical models of the hardware, OS and IDE can exhibit non-linearity. Also, the study is made with the assumption that all the elements are at their steady-states. The dynamic factors, such as hardware and software ageing should also be taken into account, regardless of the reliability and availability values prescribed in the respective safety certificates. In the thesis, the code portabilities of different third-party IDEs to the concerned OS platforms are discussed and graded. In that analysis, it has been observed that applications from FlexiSafe and Prover Trident can be ported to any OS and thus these are awarded with best costs. Contrarily, SCADE does not offer any portability to QOS, and CODESYS Safety caters to only VxWorks and QNX. Therefore these two IDEs are graded poorly. This has affected the total cost of the whole platform combination. But if these third-party IDEs are not considered and the application is developed solely on the bundled IDEs offered by the alternative OS platforms, then the final cost analysis might look different. For example, the combination of CSP and VxWorks 7 along with the associated IDE, Workbench, could be a better solution than the "best" solution of MH50C, QOS and FlexiSafe, as presented in Chapter 8.5. If the project is concerned with the development of an RBC, where high-level languages, e.g. C or C++ are required to develop interfaces with interlocking systems, then there is no need to avail IEC 61131-3 language support from the third-party IDEs. Additionally, all the bundled IDEs are packed with industry-specific APIs to head-start in programming. In the thesis, Kontron's SAFe-VX platform, based on Intel Xeon processors and PikeOS, has not been considered as it is still under the certification process [126]. Also, PSS 4000-R from Pilz GmbH & Co. KG has not been surveyed, as it is a HIMA-like platform based on proprietary OS and IDE platforms [127]. Apart from these, the thesis does not consider the possible migration policies of the proposed alternative platforms. This is an important factor in assigning costs to each combination. The product prices are not included in the thesis to respect the non-disclosure agreements. In reality, the price vs. performance trade-off would be one of the important conclusive parameters. Furthermore, unquantifiable factors, such as organizational vision in terms of project demands, application developers' willingness to go past the learning curve and get accustomed with a new software platform, legal issues associated with importing products of non-EU origin, etc. should also be taken into account. The idea of an open control system can be challenged by the fact there would be a lot of things to be taken care of in case the hardware, OS, and IDE platforms are from different suppliers with different life-cycle issues. Especially, the system integrators are less concerned about the OS, as Don Ulrich of Stone Technologies have summed it up by commenting "We don't care what OS is in a Siemens controller for instance - the customer goes back to the vendor.

People are happy to have PLCs (especially for larger systems), happy to have GE, Schneider, etc. because the long-term maintainability is done by them." [128].

The thesis has pointed out that the limited memory capacity of the present platform is one of the motivations to investigate for a new platform. But from the comparative analysis performed in the thesis, which is a hypothetical guesstimate from the respective product descriptions, it is not possible to figure out about the amount of usable memory that would be available in the CSP or MH50C platform after installing a particular OS. Therefore, the future work involves, acquiring test-beds from the hardware, operating system, and development environment vendors; developing and executing sample applications; and comparing the results with the present HIMA platform benchmarks, such as total execution time and memory consumption of a program and the related data. These variables decide the number of CPUs required for a particular interlocking application. Once a specific platform is chosen, migration policies from the hardware and software perspectives need to be devised. It is also of special interest to check whether the selected components conform to the ERTMS, EULYNX and RCA baselines.

References

[1] European Commission. (2008). *Modern rail modern Europe: Towards an integrated European railway area.* Available at https://ec.europa.eu/transport/sites/transport/files/media/publications/doc/modern_rail_en.pdf. [Accessed: 11.06.2019].

[2] Dionori, F., Casullo, L., Ellis, S., Ranghetti, D., Bablinski, K., Vollath, C. & Soutra, C. (2015). *Freight on road: Why EU shippers prefer truck to train.* Available at https://www.europarl.europa.eu/RegData/etudes/STUD/2015/540338/IPOL_STU(2015)540338_EN.pdf. [Accessed: 12.06.2019].

[3] Väylä. (2019). *Trans-European Transport Network TEN-T.* Available at https://vayla.fi/web/en/transport-system/ten-t. [Accessed: 13.06.2019].

[4] European Commission. (2017). *Trans-European Transport Network: TEN-T Core Network Corridors.* Available at https://ec.europa.eu/transport/infrastructure/tentec/tentec-portal/site/maps_upload/SchematicA0_EUcorridor_map.pdf. [Accessed: 13.06.2019].

[5] Väylä. (2014). *EU:n päätös kattavaksi verkoiksi.* Available at https://vayla.fi/documents/20473/469556/TEN_T_ydinverkon_kartat_022014.pdf/3ed60a82-42cf-414d-bb82-de6b4beb1da9.[Accessed: 13.06.2019].

[6] Josserand, P. (1957). *Rights of trains* (5th ed.). Simmons-Boardman Publishing.

[7] Finnish Transport Agency. (2012). *Signalling Systems: RATO 6.* Available at http://www2.liikennevirasto.fi/julkaisut/pdf3/2012_rato6_en_web.pdf. [Accessed: 03.07.2019].

[8] Finnish Transport Agency. (2010). *Finnish Interlocking Requirements 2010: Functional Requirements v1.4.* Available at https://julkaisut.liikennevirasto.fi/pdf4/fir_2010_functional_requirements_v1.4_web.pdf. [Accessed: 03.07.2019].

[9] Finnish Transport Agency. (2010). *Finnish Interlocking Requirements 2010: Qualitative Requirements v1.2.* Available at https://julkaisut.vayla.fi/pdf4/fir_2010_qualitative_requirements_v1.2_web.pdf. [Accessed: 03.07.2019].

[10] Finnish Transport Agency. (2014). *ATP-VR/RHK Encoder Requirements Specification.* Available at https://julkaisut.liikennevirasto.fi/pdf8/ohje_2014_atp_encoder_web.pdf. [Accessed: 04.07.2019].

[11] Väylä. (2019). *Network Statement 2019.* Available at https://vayla.fi/web/network-statement-2019/report. [Accessed: 08.07.2019].

[12] Finnish Transport Agency. (2014). *Finnish Interlocking Requirements 2010: Qualitative Requirements v1.1: Appendix 2 – Juridical Recorder*. Available at https://julkaisut.liikennevirasto.fi/pdf4/fir_2010_juridical_recorder.pdf. [Accessed: 04.07.2019].

[13] Sommerville, I. (2016). *Software Engineering* (10th ed.). Boston: Pearson Education Limited.

[14] IEC. (2010). *IEC 61508: 2010, Functional safety of electrical/electronic/ programmable electronic safety-related systems*. IEC, Geneva, Switzerland.

[15] Storey, N. (1996). *Safety-critical Computer Systems* (Repr.). New York: Addison-Wesley.

[16] CENELEC. (2017). *EN 50126: 2017, Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)*. CENELEC Management Centre, Brussels.

[17] CENELEC. (2011). *EN 50128: 2011, Railway Applications - Communication, signalling and processing systems - Software for railway control and protection systems*. CENELEC Management Centre, Brussels.

[18] CENELEC. (2018). *EN 50129: 2018, Railway Applications - Communication, signalling and processing systems - Safety related electronic systems for signalling*. CENELEC Management Centre, Brussels.

[19] Myklebust, T. & Stålhane, T. (2018). *The Agile Safety Case*. Cham: Springer.

[20] CENELEC. (2010). *EN 50159: 2010, Railway Applications - Communication, signalling and processing systems - Safety-related communication in transmission systems*. CENELEC Management Centre, Brussels.

[21] EUG. *MEMBERS*. Available at https://ertms.be/members. [Accessed: 11.09.2019].

[22] Wikipedia. *Radio Block Centre*. Available at https://de.wikipedia.org/wiki/Radio_Block_Centre. [Accessed: 12.09.2019].

[23] UNISIG. (2015). *Subset-037: EuroRadio FIS*. Available at https://www.era.europa.eu/sites/default/files/filesystem/ertms/ccs_tsi_annex_a_-_mandatory_specifications/set_of_specifications_3_etcs_b3_r2_gsm-r_b1/index010_-_subset-037_v320.pdf. [Accessed: 12.09.2019].

[24] UNISIG. (2012). *Subset-098: RBC-RBC Safe Communication Interface*. Available at https://www.era.europa.eu/sites/default/files/filesystem/ertms/ccs_tsi_annex_a_-_mandatory_specifications/set_of_specifications_3_etcs_b3_r2_gsm-r_b1/index063_-_subset-098_v300.pdf. [Accessed: 12.09.2019].

[25] European Commission. (2019). *ERTMS - Levels and Modes*. Available at https://ec.europa.eu/transport/modes/rail/ertms/what-is-ertms/levels_and_modes_en. [Accessed: 14.09.2019].

[26] UNIFE. (2019). *ERTMS Signalling Levels*. Available at http://www.ertms.net/?page_id=42. [Accessed: 14.09.2019].

[27] Pylvänäinen, J., Lehtola, J., Nieminen, T., Brotherus, M., Sandelin, E., Wallin, J. & Artukka, J. (2020). *Kohti digitaalista ja älykästä rautatieliikennettä – Digirata-selvityksen loppuraportti. Liikenne- ja viestintäministeriön julkaisuja 2020:6*. Available at http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162151/LVM_2020_6.pdf?sequence=1&isAllowed=y. [Accessed: 16.04.2020].

[28] Briginshaw, D. (2015). *Get ready for the next signalling revolution*. International Railway Journal, 55(10), p. 4. Available at https://www.railjournal.com/opinion/get-ready-for-the-next-signalling-revolution. [Accessed: 15.09.2019].

[29] EULYNX. *Landing Page*. Available at https://eulynx.eu/index.php. [Accessed: 15.09.2019].

[30] EULYNX. *International Knowledge Cooperation*. Available at https://eulynx.eu/index.php/news/47-international-knowledge-cooperation. [Accessed: 15.09.2019].

[31] EULYNX. *EULYNX System definition: Appendix A1 - EULYNX System architecture*. Available at https://eulynx.eu/index.php/documents/published-documents/open-availability/baseline-set-3/247-20191202-eulynx-system-definition-appendix-a1-eu-doc-7-a1-v3-2-0-a/file. [Accessed: 19.09.2019].

[32] Schwencke, D., Hungar, H. & Caspar, M. (2017). *Between Academics and Practice: Model-based Development of Generic Safety-Critical Systems*. Modellbasierte Entwicklung eingebetteter Systeme. Available at https://elib.dlr.de/117338/1/paper.pdf. [Accessed: 15.09.2019].

[33] EUG & EULYNX. (2018). *White Paper Reference CCS Architecture based on ERTMS*. Available at https://ertms.be/sites/default/files/2018-09/18C044_1_White_Paper_Reference_CCS_Architecture.pdf. [Accessed: 19.09.2019].

[34] EUG & EULYNX. (2020). *RCA Gamma: RCA Architecture Poster*. Available at https://public.3.basecamp.com/p/yc5xFvnXV8fe19kkEPDkQvjS. [Accessed: 20.03.2020].

[35] EUG & EULYNX. (2019). *RCA Alpha: Architecture Overview*. Available at https://ertms.be/sites/default/files/2019-08/RCA_Alpha_Architecture_Overview.pdf. [Accessed: 20.03.2020].

[36] Mipro Oy. (2018). *PRO-019446: Mipro TCS-O System Architecture Specification.* [Accessed: 07.05.2019].

[37] Mipro Oy. (2011). *TUO-000769: MISO TCS-O Platform.* [Accessed: 08.05. 2019].

[38] Mipro Oy. (2018). *TUO-002286: Mipro TCS-O Hardware Architecture.* [Accessed: 13.05.2019].

[39] HIMA Paul Hildebrandt GmbH. (2015). *HIMax Brochure.* Available at https://www.hima.com/index.php?eID=dumpFile&t=f&f=3937&token=b93da1693f8163f705ff852997fa819e40cc0b4e. [Accessed: 15.05.2019].

[40] HIMA Paul Hildebrandt GmbH. (2019). *HIMax Safety Manual.* Available at https://www.hima.com/en/extranet/quick-links/index.php?eID=dumpFile&t=f&f=PU00008759&token=dbe81b52eeb6d1540d0d3e0fc43e7a1908d4d0c9. [Accessed: 15.05.2019].

[41] HIMA Paul Hildebrandt GmbH. (2019). *HIMax: X-SB 01 System Bus Module Manual.* Available at https://www.hima.com/en/extranet/quick-links/index.php?eID=dumpFile&t=f&f=PU00008760&token=20920d9bb8cde34c318dce82587d0813c5510261. [Accessed: 15.05.2019].

[42] HIMA Paul Hildebrandt GmbH. (2019). *HIMax: X-CPU 01 Processor Module Manual.* Available at https://www.hima.com/en/extranet/quick-links/index.php?eID=dumpFile&t=f&f=PU00008761&token=167563e2289370a6fe7ffca905c415f6a37c60d2. [Accessed: 17.05.2019].

[43] HIMA Paul Hildebrandt GmbH. (2019). *HIMax: X-CPU 31 Processor Module Manual.* Available at https://www.hima.com/en/extranet/quick-links/index.php?eID=dumpFile&t=f&f=PU00010181&token=fc5bf54c6494b107a04c813297814d92576f1636. [Accessed: 17.05.2019].

[44] HIMA Paul Hildebrandt GmbH. (2013). *HIMax: X-COM 01 Communication Module Manual.* Available at https://www.hima.com/en/extranet/quick-links/index.php?eID=dumpFile&t=f&f=PU00008762&token=b37595cc90ee116232e9299904943d631be46575. [Accessed: 20.05.2019].

[45] HIMA Paul Hildebrandt GmbH. (2018). *HIMatrix F35 03 Manual.* Available at https://www.hima.com/en/extranet/quick-links/index.php?eID=dumpFile&t=f&f=PU00008533&token=032f6de67507c30a5087070f4a573849423172d7. [Accessed: 21.05.2019].

[46] HIMA Paul Hildebrandt GmbH. (2019). *Communication Configuration in SILworX*. Available at https://www.hima.com/en/extranet/quick-links/index.php?eID=dumpFile&t=f&f=PU00008771&token=02dc9bb566f379cac370162611432f9d0039c5ce. [Accessed: 23.05.2019].

[47] HIMA Paul Hildebrandt GmbH. (2017). *X-OPC Server Manual*. Available at https://www.hima.com/en/extranet/quick-links/index.php?eID=dumpFile&t=f&f=PU00012469&token=8c810a4ae8c77ff6d5a9ab99a784ce79e3b5f447. [Accessed: 23.05.2019].

[48] HIMA Paul Hildebrandt GmbH. (2019). *Protocols: ComUserTask Manual*. Available at https://www.hima.com/en/extranet/quick-links/index.php?eID=dumpFile&t=f&f=PU00013024&token=7134cbb35b1877c1b6ab59bf669545f5037c79bd. [Accessed: 23.05.2019].

[49] Handermann, F. (2002). *Communication with SafeEthernet*. PRAXIS Profiline – Industrial Ethernet. Available at http://www.eic2.ch/pdf/SafeEthernet.pdf. [Accessed: 24.05.2019].

[50] HIMA Paul Hildebrandt GmbH. (2020). *SILworX First Steps: Programming Tool Manual*. Available at https://www.hima.com/en/extranet/quick-links/index.php?eID=dumpFile&t=f&f=PU00006946&token=ab8c3210988bb7262649daa5e6aff4b46a43d40b. [Accessed: 02.04.2020].

[51] HIMA Paul Hildebrandt GmbH. (2013). *SILworX C++ Function Block Manual*. Available at https://www.hima.com/en/extranet/quick-links/index.php?eID=dumpFile&t=f&f=PU00009642&token=e4546517abbfe0a504a50e4f55399b1f634e557d. [Accessed: 24.05.2019].

[52] Rockwell Automation. (2002). *PLC vs. Safety PLC – Fundamental and Significant Differences*. Available at http://literature.rockwellautomation.com/idc/groups/litera-ture/documents/wp/safety-wp002_-en-e.pdf. [Accessed: 03.06.2019]

[53] SMART Embedded Computing. (2020). *Company Profile*. Available at https://www.smartembedded.com/ec/about-us/company-profile. [Accessed: 11.03.2020].

[54] SMART Embedded Computing. (2020). *ControlSafe Platform Datasheet*. Available at https://www.smartembedded.com/ec/assets/smart_controlsafe_platform-ds_1582721081.pdf. [Accessed: 11.03.2020].

[55] SMART Embedded Computing. (2017). *Trends and Drivers in Fail-Safe Architectures for Rail Systems*. Available at https://www.smartembedded.com/ec/assets/cs_trends_and_drivers_wp-20oct1445392198.pdf. [Accessed: 12.03.2020].

[56] SMART Embedded Computing. (2019). *ControlSafe cIOU-DIO Module Datasheet*. Available at https://www.smartembedded.com/ec/assets/smart_ccp_dio_ds_19dec2019_1582720767.pdf. [Accessed: 12.03.2020].

[57] SMART Embedded Computing. (2019). *ControlSafe IOU-CAN Module Datasheet*. Available at https://www.smartembedded.com/ec/assets/smart_csp_can_ds_19dec2019_1582721274.pdf. [Accessed: 12.03.2020].

[58] SMART Embedded Computing. (2019). *ControlSafe IOU-UART Module Datasheet*. Available at https://www.smartembedded.com/ec/assets/smart_csp_uart_ds_19dec2019_1582721379.pdf. [Accessed: 13.03.2020].

[59] SMART Embedded Computing. (2019). *ControlSafe IOU-ETH Module Datasheet*. Available at https://www.smartembedded.com/ec/assets/smart_csp_ethernet_ds_19dec2011582721323.pdf. [Accessed: 13.03.2020].

[60] SMART Embedded Computing. (2020). *ControlSafe Expansion Box Platform Datasheet*. Available at https://www.smartembedded.com/ec/assets/smart_controlsafe_exb_platform1582721034.pdf. [Accessed: 13.03.2020].

[61] SMART Embedded Computing. (2020). *ControlSafe Carborne Platform Datasheet*. Available at https://www.smartembedded.com/ec/assets/smart_controlsafe_carborne_pla1582720976.pdf. [Accessed: 13.03.2020].

[62] TÜV SÜD Product Service GmbH. (2016). *Certificate No. Z10 16 08 87324 008*. Available at https://www.smartembedded.com/ec/assets/z10_16_08_87324_008_1472165697.pdf. [Accessed: 13.03.2020].

[63] SMART Embedded Computing. (2020). *Solution Services*. Available at https://www.smartembedded.com/ec/products/solution-services. [Accessed: 16.03.2020].

[64] Artesyn Embedded Technologies. (2018). *Case Study: Artesyn's collaboration with China Railway Signal & Communication Corporation Limited*. Available at https://www.smartembedded.com/ec/assets/crsc_use_case_07aug2018_en_1536157989.pdf. [Accessed: 16.03.2020].

[65] Artesyn Embedded Technologies. (2018). *Case Study: Artesyn's Collaboration with Hyukshin Engineering Company Limited*. Available at https://www.smartembedded.com/ec/assets/hyukshin_use_case_03sep2018_en1536158269.pdf. [Accessed: 16.03.2020].

[66] duagon AG. *Brochure*. Available at https://www.men.de/fileadmin/user_upload/content_images/corporate/duagon-image-brochure-web.pdf. [Accessed: 25.03.2020].

[67] MEN Mikro Elektronik GmbH. (2018). *MH50C Data Sheet*. Available at https://www.men.de/loadfile.php?t=2&f=mh50c-data-sheet.pdf. [Accessed: 22.07.2019].

[68] MEN Mikro Elektronik GmbH. (2020). *F75P Data Sheet*. Available at https://www.men.de/loadfile.php?t=2&f=f75p-data-sheet.pdf. [Accessed: 25.03.2020].

[69] EtherCAT Technology Group. (2018). *EtherCAT Brochure*. Available at https://www.ethercat.org/download/documents/ETG_Brochure_EN.pdf. [Accessed: 22.07.2019].

[70] MEN Mikro Elektronik GmbH. (2017). *menTCS – Modular Control System: Frequently Asked Questions*. Available at https://www.men.de/loadfile.php?t=2&f=20mtcs-01_faqs.pdf. [Accessed: 22.07.2019].

[71] MEN Mikro Elektronik GmbH. (2017). *menTCS – MEN Train Control System: Brochure*. Available at https://www.men.de/loadfile.php?t=2&f=men-train-control-system-brochure-web.pdf. [Accessed: 22.07.2019].

[72] MEN Mikro Elektronik GmbH. (2018). *K2 Data Sheet*. Available at https://www.men.de/loadfile.php?t=2&f=k2-data-sheet.pdf. [Accessed: 23.07.2019].

[73] MEN Mikro Elektronik GmbH. (2018). *K1 Data Sheet*. Available at https://www.men.de/loadfile.php?t=2&f=k1-data-sheet.pdf. [Accessed: 23.07.2019].

[74] MEN Mikro Elektronik GmbH. (2018). *K7 Data Sheet*. Available at https://www.men.de/loadfile.php?t=2&f=k7-data-sheet.pdf. [Accessed: 23.07.2019].

[75] MEN Mikro Elektronik GmbH. (2018). *KT8 Data Sheet*. Available at https://www.men.de/loadfile.php?t=2&f=kt8-data-sheet.pdf. [Accessed: 23.07.2019].

[76] TÜV SÜD Product Service GmbH. *Product Service Certificate Explorer*. Available at https://www.tuvsud.com/en/services/product-certification/ps-cert. [Accessed: 02.04.2020].

[77] MEN Mikro Elektronik GmbH. (2020). *F75P - Vital Embedded Single Board Computer, 3 Intel Atom E6xx*. Available at https://www.men.de/products/cpu-boards-1/f75p/. [Accessed: 02.04.2020].

[78] MEN Mikro Elektronik GmbH. (2016). *F75P Railway Certification Packages*. Available at https://www.men.de/loadfile.php?t=2&f=f75p-certification-packages.pdf. [Accessed: 24.07.2019].

[79] MEN Mikro Elektronik GmbH. (2020). *Technology Partners*. Available at https://www.menmicro.com/corporate/technology-partners/. [Accessed: 02.04.2020].

[80] Silberschatz, A., Galvin, P. & Gagne, G. (2008). *Operating System Concepts* (8th ed.). John Wiley & Sons.

[81] Wind River Systems, Inc. (2018). *Wind River to be Acquired by TPG*. Available at https://www.windriver.com/news/press/pr.html?ID=20982. [Accessed: 09.09.2019].

[82] Wind River Systems, Inc. (2019). *VxWorks 7 Datasheet*. Available at https://www.windriver.com/products/documents/vxworks-7-datasheet/vxworks-7-datasheet.pdf. [Accessed: 09.09.2019].

[83] TÜV SÜD Product Service GmbH. (2019). *Certificate No. Z10 075658 0005 Rev. 01*. Available at https://www.windriver.com/announces/vxworks-cert-edition-regulatory-approval-IEC-62304-for-medical/documents/TUV-certificate-075658-0005.pdf. [Accessed: 10.09.2019].

[84] Wind River Systems, Inc. (2017). *Wind River VxWorks 653 Platform Product Overview*. Available at https://www.windriver.com/products/product-overviews/vxworks-653-product-overview/vxworks-653-product-overview.pdf. [Accessed: 09.09.2019].

[85] Wind River Systems, Inc. (2015). *Wind River Workbench 3.3 Datasheet*. Available at https://www.windriver.com/products/product-notes/PN_Workbench_0611/PN_Workbench_0611.pdf. [Accessed: 11.09.2019].

[86] Wind River Systems, Inc. (2018). *Wind River DIAB Compiler TÜV Certification*. Available at https://www.windriver.com/products/development-tools/Diab-TUEVCertificate/Diab-TUEVCert.pdf?v3. [Accessed: 11.09.2019].

[87] Wind River Systems, Inc. (2011). *Wind River and Beijing Traffic Control Technology Collaborate to Develop Advanced Subway Train Control System*. Available at https://www.windriver.com/news/press/pr.html?ID=9121. [Accessed: 12.09.2019].

[88] Wind River Systems, Inc. (2015). *LSIS Accelerates Delivery of Smart Train Control System with Comprehensive Wind River Solution*. Available at https://www.windriver.com/news/press/pr.html?ID=13718. [Accessed: 12.09.2019].

[89] BlackBerry Limited. (2020). *About BlackBerry QNX*. Available at https://blackberry.qnx.com/en/company/about-qnx#blackberry-qnx. [Accessed: 06.04.2020].

[90] BlackBerry Limited. (2019). *Product Brief: QNX OS for Safety*. Available at http://blackberry.qnx.com/content/dam/qnx/products/certified_os/qnx-os-for-safety-gem-2-print-product-brief-v5.pdf. [Accessed: 13.08.2019].

[91] BlackBerry Limited. (2017). *Product Brief: QNX Neutrino Realtime Operating System*. Available at http://blackberry.qnx.com/content/dam/qnx/products/neutrino-rtos/qnx-neutrino-product-brief.pdf. [Accessed: 13.08.2019].

[92] TÜV Rheinland Industrie Service GmbH. (2015). *Certificate No.: 968/EZ 653.01/15*. Available at https://www.certipedia.com/fs-products/files/certificates/certificates_asi/2015/EZ/968_EZ_653_01_15/968_EZ_653_01_15_en_el.pdf. [Accessed: 14.08.2019].

[93] BlackBerry Limited. (2019). *Product Brief: QNX Hypervisor for Safety*. Available at https://blackberry.qnx.com/content/dam/qnx/v3/hypervisor/QNX_HypervisorAutomotive_ProductBrief_2019_v8.pdf. [Accessed: 22.08.2019].

[94] BlackBerry Limited. (2017). *Product Brief: QNX Momentics Tool Suite*. Available at http://blackberry.qnx.com/content/dam/qnx/products/tools/qnx-momentics-product-brief.pdf. [Accessed: 23.08.2019].

[95] Green Hills Software. (2020). *About Us*. Available at https://www.ghs.com/corporate/index.html. [Accessed: 15.01.2020].

[96] Green Hills Software. (2020). *INTEGRITY Real-Time Operating System*. Available at https://www.ghs.com/products/rtos/integrity.html. [Accessed: 15.01.2020].

[97] exida. (2019). *Certificate No.: GHS 1105010 C001*. Available at https://www.exida.com/2019/GHS_11-05-010_C001_V2R2_61508_Certificate_-_INTEGRITY_OS.pdf. [Accessed: 17.01.2020].

[98] exida. (2019). *Certificate No.: GHS 1105010 C002*. Available at https://www.exida.com/2019/GHS_11-05-010_C001_V2R2_61508_Certificate_-_INTEGRITY_OS.pdf. [Accessed: 17.01.2020].

[99] Green Hills Software. (2020). *MULTI Integrated Development Environment Datasheet*. Available at http://www.ghs.com/download/datasheets/MULTI.pdf. [Accessed: 21.01.2020].

[100] exida. (2019). *Certificate No.: GHS 1309036 C001*. Available at https://www.exida.com/2019/GHS_13-09-036_C001_V5R4_Tool_Qual_-_MULTI.pdf. [Accessed: 17.01.2020].

[101] Green Hills Software. (2020). *Green Hills Software Customer Gallery*. Available at https://www.ghs.com/CustomerGallery.html?tab=industry. [Accessed: 21.01.2020].

[102] SYSGO GmbH. *About SYSGO: Company Profile*. Available at https://www.sysgo.com/company/about-sysgo/company-profile. [Accessed: 25.02.2020].

[103] SYSGO GmbH. (2020). *SYSGO Product Overview: PikeOS 5*. Available at https://www.sysgo.com/fileadmin/user_upload/www.sysgo.com/redaktion/downloads/pdf/data-sheets_certificates/SYSGO_PikeOS_5_Product_Overview.pdf. [Accessed: 26.02.2020].

[104] SYSGO GmbH. (2020). *PikeOS EN 50128 Certification Kit*. Available at https://www.sysgo.com/fileadmin/user_upload/www.sysgo.com/redaktion/downloads/pdf/data-sheets_certificates/SYSGO_EN50128_Certification_Kit.pdf. [Accessed: 26.02.2020].

[105] SYSGO GmbH. (2020). *SYSGO Product Overview: CODEO*. Available at https://www.sysgo.com/fileadmin/user_upload/www.sysgo.com/redaktion/downloads/pdf/data-sheets_certificates/SYSGO_Product_Overview_CODEO.pdf. [Accessed: 27.02.2020].

[106] SYSGO GmbH. (2020). *SYSGO Customer Success Overview*. Available at https://www.sysgo.com/fileadmin/user_upload/www.sysgo.com/redaktion/downloads/pdf/use-cases/SYSGO-Success-Story-MEN.pdf. [Accessed: 27.02.2020].

[107] Jack, H. (2008). *Automating Manufacturing Systems with PLCs*. Version 5.1. Available at https://archive.org/details/ost-engineering-plcbook5_1. [Accessed: 24.10.2019].

[108] Vyatkin, V. (2016). *IEC 61499 function blocks for embedded and distributed control systems design* (3rd ed.). Research Triangle Park, NC: ISA.

[109] ANSYS, Inc. (2020). *About Ansys*. Available at https://www.ansys.com/about-ansys. [Accessed: 12.02.2020].

[110] Colaco, J., Pagano, B. & Pouzet, M. (2017). *SCADE 6: A formal language for embedded critical software development (invited paper)*. Available at https://www.di.ens.fr/~pouzet/bib/tase17.pdf. [Accessed: 23.07.2019].

[111] Colaco, J., Pagano, B., Pasteur, C. & Pouzet, M. (2018). *Scade 6: From a Kahn Semantics to a Kahn Implementation for Multicore*. Available at https://hal.archives-ouvertes.fr/hal-01960410/document. [Accessed: 23.07.2019].

[112] ANSYS, Inc. (2019). *SCADE Suite 2019 R1 Datasheet*. Available at https://www.ansys.com/-/media/ansys/corporate/resourcelibrary/brochure/scade-suite-datasheet-2019-r1.pdf. [Accessed: 23.07.2019].

[113] Ansys (2015, August 5). *CASCO Signalling Company and ANSYS [Case Study]*. [Video File]. Retrieved from https://youtu.be/0-kBuhTzDow.

[114] infoteam Software AG. *About infoteam Software AG*. Available at https://infoteam.de/en/company/. [Accessed: 20.11.2019].

[115] Rockwell Automation, Inc. (2020). *ISaGRAF Technology*. Available at https://www.rockwellautomation.com/global/detail.page?pagetitle=Isagraf&content_type=tech_data&docid=209076c017d6dd586c895e9e3a4856e4&redirect_type=tld&redirect_url=www.isagraf.com. [Accessed: 15.04.2020].

[116] infoteam Software AG. (2016). *Datasheet: FlexiSafe*. Available at https://infoteam.de/en/our-know-how/plc-programming-systems/. [Accessed: 20.11.2019].

[117] TÜV Rheinland Industrie Service GmbH. (2015). *Certificate No.: 968/EZ 552.03/17*. Available at https://www.certipedia.com/fs-products/files/certificates/certificates_asi/2017/EZ/968_EZ_552_03_17/968_EZ_552_03_17_en_el.pdf. [Accessed: 15.04.2020].

[118] infoteam Software AG. (2014). *Whitepaper: iFSC - infoteam Functional Safety Control Concept*. Available at https://infoteam.de/en/our-know-how/functional-safety/. [Accessed: 21.11.2019].

[119] FIORD Company. (2020). *ISaGRAF in railway transport worldwide*. Available at https://isagraf.ru/images/industry_avt/soft/isagraf/ISaGRAF%20and%20railways.pdf. [Accessed: 15.04.2020].

[120] Prover Technology AB. *About us*. Available at https://www.prover.com/about-us/. [Accessed: 27.08.2019].

[121] Prover Technology AB. *Prover Trident*. Available at https://www.prover.com/software-solutions-rail-control/prover-trident/. [Accessed: 27.08.2019].

[122] Prover Technology AB. *Prover iLock*. Available at https://www.prover.com/software-solutions-rail-control/prover-ilock/. [Accessed: 28.08.2019].

[123] Prover Technology AB. *References*. Available at https://www.prover.com/references/. [Accessed: 28.08.2019].

[124] 3S-Smart Software Solutions GmbH. (2016). *CODESYS Safety*. Available at https://www.codesys.com/fileadmin/data/Downloads/Broschueren/CODESYS-Safety-en.pdf. [Accessed: 18.09.2019].

[125] TÜV Rheinland Industrie Service GmbH. (2017). *Certificate No.: 968/EZ 568.10/17*. Available at https://www.certipedia.com/fs-products/files/certificates/certificates_asi/2017/EZ/968_EZ_568_10_17/968_EZ_568_10_17_en_el.pdf. [Accessed: 18.09.2020].

[126] Kontron S&T AG. (2019). *SAFe-VX Datasheet*. Available at https://www.kontron.com/downloads/datasheets/safe-vx_20191025_datasheet.pdf. [Accessed: 16.01.2020].

[127] Pilz GmbH & Co. KG. *The PSS 4000-R automation system, especially for rail automation*. Available at https://www.pilz.com/en-INT/products/automation-system-pss-4000/pss-4000-r. [Accessed: 29.10.2020].

[128] Robbins, R., & Axelson, R. (2009). *When Considering Controllers...Do Operating Systems Matter?*. Available at athttps://www.controleng.com/articles/when-considering-controllers-do-operating-systems-matter/. [Accessed: 17.12.2020].

[129] TÜV SÜD Product Service GmbH. (2016). *Certificate No. Z10 16 04 19183 050*. Available at https://www.hima.com/en/extranet/quick-links/index.php?eID=dumpFile&t=f&f=PU00011786&token=83ddc004a54814ea9690748d20c4ffe46d12585f. [Accessed: 28.05.2019].

[130] TÜV SÜD Product Service GmbH. (2016). *Certificate No. Z10 16 08 19183 053*. Available at https://www.hima.com/index.php?eID=dumpFile&t=f&f=4267&token=f61ee6fe6bd32dd55dc760cfa07bc7fb41959c99. [Accessed: 28.05.2019].

[131] TÜV Rheinland Industrie Service GmbH. (2019). *Certificate No.: 968/FSP 1862.00/19*. Available at https://fs-products.tuvasi.com/files/certificates/certificates_asi/2019/FSP/968_FSP_1862_00_19/968_FSP_1862_00_19_de_en_el.pdf. [Accessed: 29.05.2019].

[132] TÜV Rheinland Industrie Service GmbH. (2015). *Certificate No.: 968/EZ 487.04/15*. Available at https://fs-products.tuvasi.com/files/certificates/certificates_asi/2015/EZ/968_EZ_487_04_15/968_EZ_487_04_15_en_el.pdf. [Accessed: 29.05.2019].

[133] TÜV Rheinland Industrie Service GmbH. (2019). *Certificate No.: 968/FSP 1976.00/19*. Available at https://www.certipedia.com/fs-products/files/certificates/certificates_asi/2019/FSP/968_FSP_1976_00_19/968_FSP_1976_00_19_en_el.pdf. [Accessed: 29.05.2019].

[134] HIMA Paul Hildebrandt GmbH. (2012). *HIMax X-DI 16 01*. Available at http://www.netmuh.com.tr/media/products/x-di-16-01_katalog77372.pdf. [Accessed: 10.09.2019].

[135] HIMA Paul Hildebrandt GmbH. (2019). *HIMax X-DI 32 01*. Available at https://www.hima.com/en/extranet/quick-links/index.php?eID=dumpFile&t=f&f=PU00008763&token=8c08e25ae2ce88d449139ca1601a5a07e9555ea1. [Accessed: 10.09.2019].

[136] HIMA Paul Hildebrandt GmbH. (2019). *HIMax X-DI 64 01*. Available at https://www.hima.com/en/extranet/quick-links/index.php?eID=dumpFile&t=f&f=PU00008793&token=a5427513ee7fce7dbbed562a2c58a3abdf0f2210. [Accessed: 10.09.2019].

[137] HIMA Paul Hildebrandt GmbH. (2019). *HIMax X-DO 12 02*. Available at https://www.hima.com/en/extranet/quick-links/index.php?eID=dumpFile&t=f&f=PU00007015&token=24708b78796013ea08048c56484558a06e0f7a75. [Accessed: 11.09.2019].

[138] HIMA Paul Hildebrandt GmbH. (2019). *HIMax X-DO 24 02*. Available at https://www.hima.com/en/extranet/quick-links/index.php?eID=dumpFile&t=f&f=PU00008796&token=79d124a85e18a450804debc699fe84586f784c3b. [Accessed: 11.09.2019].

[139] HIMA Paul Hildebrandt GmbH. (2019). *HIMax X-DO 32 01*. Available at https://www.hima.com/en/extranet/quick-links/index.php?eID=dumpFile&t=f&f=PU00008794&token=05109ce5b69f15c6a11a8310b419a66d5ca772c5. [Accessed: 11.09.2019].

[140] HIMA Paul Hildebrandt GmbH. (2019). *HIMax X-CI 24 01*. Available at https://www.hima.com/en/extranet/quick-links/index.php?eID=dumpFile&t=f&f=PU00007013&token=6b287e0d4979fb5fee8dc5403c06582dbe800f31. [Accessed: 11.09.2019].

[141] Freescale Semiconductor, Inc. (2020). *QorIQ P2010 and P2020 Processors*. Available at https://www.nxp.com/docs/en/fact-sheet/QP20XXFS.pdf. [Accessed: 19.02.2020].

[142] Freescale Semiconductor, Inc. (2013). *QorIQ P1011 and P1020 Processors*. Available at https://www.nxp.com/docs/en/fact-sheet/QorIQ_P1.pdf. [Accessed: 19.02.2020].

[143] Adiletta, M. & Mehta, P. (2010). *Tunnel Creek: Intel's First Generation Intel Atom Processor-based System-on-Chip for Embedded*. Technology Insight SPCS002. Available at http://download.intel.com/pressroom/kits/events/idfspr_2010/pdfs/Tech_Insight-Tunnel_Creek.pdf. [Accessed: 03.03.2020].

[144] Intel Corporation. (2013). *Datasheet: Intel Atom Processor E6xx Series*. Available at https://www.intel.com/content/dam/www/public/us/en/documents/datasheets/atom-e6xx-series-datasheet.pdf. [Accessed: 21.02.2020].

[145] MEN Mikro Elektronik GmbH. (2019). *F305 Data Sheet*. Available at https://www.men.de/loadfile.php?t=2&f=f305-data-sheet.pdf. [Accessed: 20.08.2019].

[146] MEN Mikro Elektronik GmbH. (2018). *PU20 Data Sheet*. Available at https://www.men.de/loadfile.php?t=2&f=pu20-data-sheet.pdf. [Accessed: 20.08.2019].

[147] Wind River Systems, Inc. (2020). *Board Support Packages: VxWorks 7 BSP for NXP QorIQ P1/P2 family*. Available at https://marketplace.windriver.com/index.php?bsp&on=details&bsp=12931. [Accessed: 15.04.2020].

[148] Wind River Systems, Inc. (2020). *VxWorks 7 Unified BSP for Intel Architectures*. Available at https://marketplace.windriver.com/index.php?bsp&on=details&bsp=12944. [Accessed: 15.04.2020].

[149] QNX Software Systems. (2013). *BSPs and Drivers: Freescale P2020RDB-PCA Board Support Package*. Available at http://community.qnx.com/sf/wiki/do/viewPage/projects.bsp/wiki/FreescaleP2020rdbPca. [Accessed: 25.03.2020].

[150] QNX Software Systems. (2011). *BSPs and Drivers: Intel Crown Bay Board Support Package*. Available at http://community.qnx.com/sf/wiki/do/viewPage/projects.bsp/wiki/Bspdown_crownbay. [Accessed: 25.03.2020].

[151] Green Hills Software. (2020). *INTEGRITY RTOS Board Support Packages (BSPs)*. Available at https://www.ghs.com/products/rtos/board_support_packages.html. [Accessed: 13.03.2020].

[152] SYSGO GmbH. *PikeOS BSP List*. Available at https://www.sysgo.com/products/board-support-packages/pikeos-bsp-list. [Accessed: 10.04.2020].

[153] TÜV SÜD Product Service GmbH. (2017). *Certificate No. Z10 17 09 87324 012*. Available at https://www.smartembedded.com/ec/assets/z10_17_09_87324_012_-_farbe_1531796134.pdf. [Accessed: 22.01.2020].

[154] TÜV SÜD Product Service GmbH. (2016). *Certificate No. Z10 16 10 87324 011*. Available at https://www.smartembedded.com/ec/assets/z10_16_10_87324_011_1476744676.pdf. [Accessed: 22.01.2020].

A Certifications

The nature and validity of certifications of all the products discussed in the thesis, have been thoroughly checked from the certification agencies' databases. This section presents only the publicly accessible certification copies of the products discussed in the thesis.

A.1 HIMA

HIMax

The following illustrates certification of HIMax system according to EN 50126: 1999 (SIL 4), EN 50128: 2011 (SIL 4), EN 50129: 2003 (SIL 4) and EN 50159: 2010 by TÜV SÜD.

ZERTIFIKAT ◆ CERTIFICATE ◆ 認證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

TÜV SÜD Product Service

CERTIFICATE

No. Z10 16 04 19183 050

Holder of Certificate: HIMA Paul Hildebrandt GmbH
Albert-Bassermann-Str. 28
68782 Brühl
GERMANY

Factory(ies): 19183

Certification Mark:

Product: Safety-Related Programmable Systems

Model(s): HIMax

Parameters: Operational voltage: 24VDC -20% +25%
The actual versions of the test report listed below and of the user manual are mandatory part of this certificate.

Tested according to:
EN 50126:1999 (SIL4)
EN 50129:2003 (SIL4)
EN 50128:2011 (SIL4)
EN 50159:2010
EN 50122-1:2011
EN 50124-1:2001/A2:2005
EN 50125-1:2014
EN 50121-4:2015
EN 50125-3:2003
EN 50155:2007

The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition the certification holder must not transfer the certificate to third parties. See also notes overleaf.

Test report no.: HM83594T

Valid until: 2021-05-03

Date, 2016-05-04 (Peter Weiss)

Page 1 of 1

TÜV SÜD Product Service GmbH · Zertifizierstelle · Ridlerstraße 65 · 80339 München · Germany TÜV®

Figure A1: HIMax SIL certification [129].

HIMatrix

The following illustrates certification of HIMatrix system according to EN 50126: 1999 (SIL 4), EN 50128: 2011 (SIL 4) and EN 50129: 2003 (SIL 4) by TÜV SÜD.

ZERTIFIKAT ◆ CERTIFICATE ◆ 認証書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

Product Service

CERTIFICATE

No. Z10 16 08 19183 053

Holder of Certificate: HIMA Paul Hildebrandt GmbH
Albert-Bassermann-Str. 28
68782 Brühl
GERMANY

Factory(ies): 19183

Certification Mark:

Product: Safety-Related Programmable Systems

Model(s): HIMatrix F30, HIMatrix F35, HIMatrix F60, HIMatrix Remote I/O

Parameters: Operating voltage: 24 VDC -20% +25%

Tested according to:
EN 50126:1999 SIL4
EN 50129:2003 SIL4
EN 50128:2011 SIL4
IEC 61508-1(ed.2) SIL3
IEC 61508-2(ed.2) SIL3
IEC 61508-3(ed.2) SIL3
IEC 61508-4(ed.2) SIL3

The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition the certification holder must not transfer the certificate to third parties. See also notes overleaf.

Test report no.: HB82132C

Valid until: 2021-08-09

Date, 2016-08-10 (Peter Weiss)

Page 1 of 1

TÜV SÜD Product Service GmbH · Zertifizierstelle · Ridlerstraße 65 · 80339 München · Germany TÜV®

Figure A2: HIMax SIL certification [130].

SILworX

The following illustrates certification of SILworX IDE by TÜV Rheinland, as per the requirements set by IEC 61508-3: 2010 for tool class T3.

Certificate

Functional Safety

TÜVRheinland CERTIFIED

www.tuv.com
ID 0600000000

Nr./No.: 968/FSP 1862.00/19

Prüfgegenstand **Product tested**	Programmier- und Konfigurationswerkzeug für sicherheitsbezogene programmierbare elektronische Systeme. Programming- and configuration tool for safety related programmable electronic systems.	**Zertifikats-inhaber** **Certificate holder**	HIMA Paul Hildebrandt GmbH Albert-Bassermann-Str. 28 68782 Brühl Germany
Typbezeichnung **Type designation**	SILworX (siehe Revisionliste /see Revisionslist)		
Prüfgrundlagen **Codes and standards**	IEC 61508 Parts 1-7:2010 (in extracts)		
Bestimmungsgemäße Verwendung **Intended application**	Das Programmierwerkzeug SILworX erfüllt die Anforderungen für ein Offline-Werkzeug der Klasse T3 gemäß IEC 61508-3. The programming tool SILworX meets the requirements for offline-tools of class T3 according to IEC 61508-3.		
Besondere Bedingungen **Specific requirements**	SILworX kann für die Erstellung von Anwenderprogrammen und die Konfiguration der sicherheitsbezogenen programmierbaren elektronischen Systeme HIMax, HIMatrix F-Serie und HIQuad X verwendet werden. Die aktuellen Versionen der Produkte sind in den dazugehörigen Revisionsliste dokumentiert, die vom Hersteller in Kooperation mit der Zertifizierungsstelle freigegeben werden. Die Hestellerdokumentation ist zu beachten. SILworX can be used to create user programs and configure the safety-related programmable electronic systems HIMax, HIMatrix F-Series and HIQuad X. The current versions of the products are documented in the belonging revision list, which are released by the manufacturer in cooperation with the certification body. The manufacturer documentation needs to be considered.		

Gültig bis / Valid until 2024-09-03

Der Ausstellung dieses Zertifikates liegt eine Prüfung zugrunde, deren Ergebnisse im Bericht Nr. 968/FSP 1862.00/19 vom 03.09.2019 dokumentiert sind.
Dieses Zertifikat ist nur gültig für Erzeugnisse, die mit dem Prüfgegenstand übereinstimmen.
The issue of this certificate is based upon an examination, whose results are documented in Report No. 968/FSP 1862.00/19 dated 2019-09-03.
This certificate is valid only for products which are identical with the product tested.

Köln, 2019-09-03

TÜV Rheinland Industrie Service GmbH
Bereich Automation
Funktionale Sicherheit
Am Grauen Stein, 51105 Köln
Certification Body Safety & Security for Automation & Grid

Dipl.-Ing. Thomas Steffens

TÜV Rheinland Industrie Service GmbH, Am Grauen Stein, 51105 Köln / Germany
Tel.: +49 221 806-1790, Fax: +49 221 806-1538, E-Mail: industrie-service@de.tuv.com

www.fs-products.com
www.tuv.com

TÜVRheinland®
Precisely Right.

Figure A3: SILworx IDE certification [131].

The following illustrates certification of SILworX functon block library, by TÜV Rheinland. This library can be used for SIL 3 applications according to IEC 61508: 2010.

Certificate

Functional Safety

TÜVRheinland CERTIFIED

www.tuv.com
ID 0000000000

No.: 968/EZ 487.04/15

Product tested	H-MO Motion Function block library for safe movement monitoring	**Certificate holder**	HIMA Paul Hildebrandt GmbH Albert-Bassermann-Str. 28 68782 Brühl bei Mannheim Germany
Type designation	Certified Function Block (CFB) H-MO Library for the SILworX programming environment, according to the current version list		
Codes and standards	IEC 61508 Parts 1-7:2010 (in extracts) EN ISO 13849-1:2008 + AC:2009		EN 62061:2005 EN 61800-5-2:2007
Intended application	SILworX function block library for HIMA safety systems HIMatrix and HIMax, developed according to IEC 61508:2010. The approved function blocks comply with the requirements of the relevant standards SIL 3 acc. to EN 62061 / IEC 61508 and PL e acc. to EN ISO 13849 and are suitable for safety related applications up to SIL 3 and PL e.		
Specific requirements	The manual (or online documentation) for each function block, that is used in the application has to be considered.		

Valid until 2020-10-23

The issue of this certificate is based upon an examination, whose results are documented in Report No. 968/EZ 487.04/15 dated 2015-10-23.
This certificate is valid only for products which are identical with the product tested. It becomes invalid at any change of the codes and standards forming the basis of testing for the intended application.

TÜV Rheinland Industrie Service GmbH
Bereich Automation
Funktionale Sicherheit
Am Grauen Stein, 51105 Köln

Köln, 2015-10-23 — Certification Body for FS-Products — Dipl.-Ing. Heinz Gall

TÜV Rheinland Industrie Service GmbH, Am Grauen Stein, 51105 Köln / Germany
Tel.: +49 221 806-0790, Fax: +49 221 806-1539, E-Mail: industrie-service@de.tuv.com

www.fs-products.com
www.tuv.com

TÜVRheinland®
Precisely Right.

Figure A4: SILworX function block certification [132].

A.2 ControlSafe Platfrom (CSP)

The following illustrates certification of the CSP and ControlSafe Software (VxWorks 653) certification according to EN 50126: 1999 (SIL 4), EN 50128: 2011 (SIL 4), EN 50129: 2003 (SIL 4) and IEC 61508: 2010 by TÜV SÜD.

ZERTIFIKAT ◆ CERTIFICATE ◆ 認証書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

Product Service

CERTIFICATE

No. Z10 16 08 87324 008

Holder of Certificate: **Artesyn Embedded Computing Inc.**
2900 South Diablo Way, Suite 190
Tempe AZ 85282
USA

Factory(ies): 26247

Certification Mark:

Product: **Safety-Related Programmable Systems**

Model(s): **ControlSafe™ Platform (CSP) with ControlSafe™ Computer (CSC) and ControlSafe™ Software**

Parameters:
Safety-related generic processing platform including:
- Safe application processing
- Voting and 2oo2 active/standby arbitration
- Safety related communication

Tested according to:
EN 50126:1999 (SIL4)
EN 50129:2003 (SIL4)
EN 50128:2011 (SIL4)
IEC 61508-1(ed.2) (SIL3)
IEC 61508-2(ed.2) (SIL3)
IEC 61508-3(ed.2) (SIL3)

The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition the certification holder must not transfer the certificate to third parties. See also notes overleaf.

Test report no.: AT88765G

Valid until: 2021-08-24

Date, 2016-08-25 (Jürgen Blum)

Page 1 of 1

TÜV SÜD Product Service GmbH · Zertifizierstelle · Ridlerstraße 65 · 80339 München · Germany

TÜV®

Figure A5: CSP SIL certification [62].

A.3 VxWorks 7

The following illustrates certification of VxWorks 7 according to IEC 61508: 2010 (SIL 3) by TÜV SÜD.

ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

Product Service

CERTIFICATE

No. Z10 075658 0005 Rev. 01

Holder of Certificate: Wind River Systems, Inc.
500 Wind River Way
Alameda CA 94501
USA

Factory(ies): 075658

Certification Mark:

Product: Software, Operating Systems
Real time Operating System

Model(s): VxWorks 7 with Safety Profile

Parameters: Safety parameters: SIL 3 (acc. to IEC 61508)
ASIL D (acc. to ISO 26262)
Class C Risk Level (acc. to IEC 62304)

The report no. WA93407C is mandatory part of the certificate. Only together with the currently valid version of the report, the product complies with the listed standards.

Tested according to:
IEC 61508-1:2010 (SIL3)
IEC 61508-3:2010 (SIL3)
IEC 61508-4:2010 (SIL3)
ISO 26262-2:2011
ISO 26262-6:2011
ISO 26262-8:2011
IEC 62304:2006
IEC 62304:2006/AMD1:2015

The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition the certification holder must not transfer the certificate to third parties. See also notes overleaf.

Test report no.: WA93407C
Valid until: 2024-09-01
Date, 2019-09-02

(Claudio Gregorio)

Page 1 of 1
TÜV SÜD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany

Figure A6: VxWorks 7 SIL certification [83].

The following illustrates certification of the proprietary DIAB compiler from Wind River by TÜV SÜD. It is used in the IDE, Workbench 3.3, bundled with VxWorks 7. The compiler fulfills the criteria of tool class T3 set by IEC 61508-3: 2010.

TIFIKAT ◆ CERTIFICATE ◆ 認証書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

Product Service

CERTIFICATE

No. Z10 17 09 75658 004

Holder of Certificate: **Wind River Systems, Inc.**
500 Wind River Way
Alameda CA 94501
USA

Factory(ies): 75658

Certification Mark:

Product: **Software Tool for Safety Related Development**

Model(s): **DIAB Compiler Toolchain**

Parameters: The development toolchain fulfils the requirements for T3 tools according to IEC 61508-3 and is qualified to be used in safety-related software development according to IEC 61508 and ISO 26262. The DIAB Compiler Toolchain can be used for any Safety Integrity Level, provided the safety component is developed in accordance with the respective requirements.

The report 2WA91503C is a mandatory part of this certificate

Tested according to: IEC 61508-3:2010
ISO 26262-8:2011

The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition the certification holder must not transfer the certificate to third parties. See also notes overleaf.

Test report no.: 2WA91503C

Valid until: 2022-08-31

Date, 2017-09-07 (Peter Weiss)

Page 1 of 1

Figure A7: WxWorks IDE SIL certification [86].

A.4 QNX OS for Safety (QOS)

The following illustrates certification of QOS and the associated toolchain according to IEC 61508: 2010 (SC 3) by TÜV Rheinland.

Certificate

Functional Safety

TÜVRheinland CERTIFIED

www.tuv.com
ID 0600000000

No.: 968/EZ 653.01/15

Product tested	Real Time Operating System (RTOS)	**Certificate holder**	QNX Software Systems Limited 1001 Farrar Road Ottawa, ON K2K 0B3 Canada
Type designation	QNX OS for Safety (QOS) for released and approved versions refer to the "Revision List"		
Codes and standards	ISO 26262 Parts 1-10:2011 (in extracts) IEC 61508 Parts 1-7:2010 (in extracts)		
Intended application	The QOS product complies with the requirements of the relevant standards (ASIL D according to ISO 26262 and SC 3 according to IEC 61508) and can be used as a Safety Element Out Of Context (SEooC) in items in order to realize safety goals up to ASIL D according to ISO 26262 and as a compliant item in applications up to SIL 3 according to IEC 61508. The provided tool chain, classified as TCL3 and T3, complies with the applicable requirements for supporting tools according to ISO 26262-8 and off-line support tools according to IEC 61508-3.		
Specific requirements	For the use of the QOS the operating conditions and functional characteristics as specified in the Safety Manual and accompanying documents provided by the manufacturer needs to be observed. The current versions of software are specified in the currently valid revision list. The list is released by the manufacturer in cooperation with the Test Institute.		

Valid until 2020-08-14

The issue of this certificate is based upon an examination, whose results are documented in Report No. 968/EZ 653.01/15 dated 2015-08-14.
This certificate is valid only for products which are identical with the product tested. It becomes invalid at any change of the codes and standards forming the basis of testing for the intended application.

Köln, 2015-08-14

TÜV Rheinland Industrie Service GmbH
Bereich Automation
Funktionale Sicherheit
Am Grauen Stein, 51105 Köln
Certification Body for FS-Products

Dipl.-Ing. Heinz Gall

TÜV Rheinland Industrie Service GmbH, Am Grauen Stein, 51105 Köln / Germany
Tel.: +49 221 806-1790, Fax: +49 221 806-1538, E-Mail: industrie-service@de.tuv.com

www.fs-products.com
www.tuv.com

TÜVRheinland®
Precisely Right.

Figure A8: QOS SIL certification [92].

The following illustrates certification of QNX Hypervisor for Safety according to IEC 61508: 2010 (SIL 3) by TÜV Rheinland.

Certificate

Functional Safety

TÜVRheinland CERTIFIED

www.tuv.com
ID 0000000000

No.: 968/FSP 1976.00/19

Product tested	Hypervisor	**Certificate holder**	QNX Software Systems Limited 1001 Farrar Road Ottawa, ON K2K 0B3 Canada
Type designation	QNX Hypervisor for Safety (QHS) for released and approved versions refer to the "Revision List"		
Codes and standards	ISO 26262 Parts 1-10:2011 (in extracts)		IEC 61508 Parts 1-7:2010 (in extracts)
Intended application	The QHS product complies with the requirements of the relevant standards (ASIL D according to ISO 26262 and SC 3 according to IEC 61508) and can be used as a Safety Element Out Of Context (SEooC) in items in order to realize safety goals up to ASIL D according to ISO 26262 and as a compliant item in applications up to SIL 3 according to IEC 61508.		
Specific requirements	For the use of the QHS the operating conditions and functional characteristics as specified in the Safety Manual and accompanying documents provided by the manufacturer need to be observed. The current versions of software are specified in the currently valid "Revision List". The list is released by the manufacturer in cooperation with the Certification Body.		

Valid until 2024-11-27

The issue of this certificate is based upon an examination, whose results are documented in Report No. 968/FSP 1976.00/19 dated 2019-11-27.
This certificate is valid only for products which are identical with the product tested.

TÜV Rheinland Industrie Service GmbH
Bereich Automation
Funktionale Sicherheit
Am Grauen Stein, 51105 Köln

Köln, 2019-11-27

Certification Body Safety & Security for Automation & Grid

Dipl.-Ing. Gebhard Bouwer

TÜV Rheinland Industrie Service GmbH, Am Grauen Stein, 51105 Köln / Germany
Tel.: +49 221 806-1790, Fax: +49 221 806-1538, E-Mail: industrie-service@de.tuv.com

www.fs-products.com
www.tuv.com

TÜVRheinland®
Precisely Right.

Figure A9: QNX Hypervisor for Safety SIL certification [133].

A.5 INTEGRITY

The following illustrates certification of INTEGRITY RTOS according to IEC 61508: 2010 (SC 3) by exida.

Figure A10: INTEGRITY RTOS SIL certification [97].

The following illustrates certification of INTEGRITY RTOS according to EN 50128: 2011 (SIL 3/4) by exida.

Figure A11: INTEGRITY RTOS SIL certification [98].

The following illustrates certification of the proprietary MULTI IDE from Green Hills Software LLC by exida. It establishes that the toolchain and runtime libraries of the IDE is certified according to IEC 61508: 2010 and EN 50128: 2011 (SIL3/4).

Figure A12: INTEGRITY IDE SIL certification [100].

A.6 FlexiSafe

The following illustrates certification of the runtime engine, workbench and PLCopen funciton block libraries in FlexiSafe. TÜV Rheinland has certified this IDE according to EN 50128: 2014 (SIL 4) and IEC 61508: 2010 (SIL 3).

Certificate

Functional Safety

TÜVRheinland CERTIFIED

www.tuv.com
ID 0600000000

No.: 968/EZ 552.03/17

Product tested	FlexiSafe Software System consisting of - FlexiSafe Run-time Engine - FlexiSafe Workbench - PLCopen Function block library	**Certificate holder**	Rockwell Automation Canada Ltd 9975 de Châteauneuf, Suite U Brossard, Quebec J4Z 3V6 Canada
Type designation	for released and approved versions refer to "Version Release List"		
Codes and standards	IEC 61508 Parts 1-7:2010 (in extracts) EN 50128:2014+ AC:2014 EN ISO 13849-1:2015 (in extracts)		
Intended application	FlexiSafe Run-time Engine comply with the applicable requirements of the relevant standards (SC3 acc. to IEC 61508, PL e acc. to EN ISO 13849-1 and SIL 4 acc. to EN 50128) and can be used in applications up to SIL 3 acc. to IEC 61508, PL e acc. to EN ISO 13849-1 and SIL 4 acc. to EN 50128. PLCopen Function blocks are developed in accordance to the PLCopen Technical Specification Part 1, V1.0, IEC 61508, SC3 and can be used in applications up to SIL 3 acc. to IEC 61508, PL e acc. to EN ISO 13849-1 and SIL 4 acc. to EN 50128. The FlexiSafe Workbench comply with the applicable requirements for off-line support tools according to IEC 61508-3.		
Specific requirements	For the use of the FlexiSafe Software System the operating conditions and functional characteristics as specified in the Safety Manual and accompanying development documents provided by the manufacturer needs to be observed. The current versions of software are specified in the currently valid version release list. The list is released by the manufacturer in cooperation with the Test Institute.		

Valid until 2022-09-11

The issue of this certificate is based upon an examination, whose results are documented in Report No. 968/EZ 552.03/17 dated 2017-09-09.
This certificate is valid only for products which are identical with the product tested. It becomes invalid at any change of the codes and standards forming the basis of testing for the intended application.

TÜV Rheinland Industrie Service GmbH
Bereich Automation
Funktionale Sicherheit
Am Grauen Stein, 51105 Köln

Köln, 2017-09-11

Certification Body Safety & Security for Automation & Grid

Dipl.-Ing. Heinz Gall

TÜV Rheinland Industrie Service GmbH, Am Grauen Stein, 51105 Köln / Germany
Tel.: +49 221 806-1792, Fax: +49 221 806-1539, E-Mail: industrie-service@de.tuv.com

www.fs-products.com
www.tuv.com

DAkkS Deutsche Akkreditierungsstelle D-ZE-11052-02-00

TÜVRheinland®
Precisely Right.

Figure A13: FlexiSafe SIL certification [117].

A.7 CODESYS Safety

The following illustrates certification of the runtime engine, workbench, funciton block libraries and fieldbus configuration in CODESYS Safety. TÜV Rheinland has certified this IDE according to IEC 61508: 2010 (SIL 3).

Certificate

Functional Safety

TÜVRheinland CERTIFIED

www.tuv.com
ID 0600000000

No.: 968/EZ 568.10/17

Product tested	Run-time System Development-Kit, Programming System incl. function block libraries and fieldbus configuration	**Certificate holder**	3S-Smart Software Solutions GmbH Memminger Str. 151 87435 Kempten Germany
Type designation	CODESYS Safety See Revision List		
Codes and standards	IEC 61508 Parts 1-7:2010 EN ISO 13849-1:2015		EN 62061:2005 + AC:2010 + A1:2013 + A2:2015
Intended application	CODESYS Safety Run-time System complies with the applicable requirements of the relevant standards (SC3 acc. to IEC 61508, PL e acc. to EN ISO 13849-1) and can be used in applications up to SIL 3 acc. to IEC 61508, EN 62061 and PL e acc. to EN ISO 13849-1. PLCopen Function blocks are developed in accordance to the PLCopen Technical Specification Part 1, V1.0, IEC 61508, SC 3 and can be used in applications up to SIL 3 acc. to IEC 61508, PL e acc. to EN ISO 13849-1. The CODESYS Programming System complies with the applicable requirements for off-line support tools of class T3 according to IEC 61508-3.		
Specific requirements	For the use of CODESYS Safety the operating conditions and functional characteristics as specified in the user manual and accompanying implementation documents by the manufacturer needs to be observed. The current versions of software are specified in the currently valid version release list. The list is released by the manufacturer in cooperation with the Test Institute.		

Valid until 2022-08-28

The issue of this certificate is based upon an examination, whose results are documented in Report No. 968/EZ 568.10/17 dated 2017-08-28.
This certificate is valid only for products which are identical with the product tested. It becomes invalid at any change of the codes and standards forming the basis of testing for the intended application.

TÜV Rheinland Industrie Service GmbH
Bereich Automation
Funktionale Sicherheit
Am Grauen Stein, 51105 Köln

Köln, 2017-08-28

Certification Body Safety & Security for Automation & Grid

Dipl.-Ing. Thomas Steffens

TÜV Rheinland Industrie Service GmbH, Am Grauen Stein, 51105 Köln / Germany
Tel.: +49 221 806-1790, Fax: +49 221 806-1539, E-Mail: industrie-service@de.tuv.com

www.fs-products.com
www.tuv.com

DAkkS Deutsche Akkreditierungsstelle D-ZE-11052-02-00

TÜVRheinland®
Precisely Right.

Figure A14: CODESYS Safety SIL certification [125].

B Datasheets

B.1 HIMA

Table B1: HIMax and HIMatrix CPU Module Datasheet.

	X-CPU 01 [42]	X-CPU 31 [43]	HIMatrix F35 03 [45]
Parameter: Processor Details			
Microprocessor	PowerPC		
Supply Voltage	24 VDC, -15...+20%		
Current Consumption	1.4 A	0.72 A	0.5 A
Parameter: Memory Details			
Dedicated Memory	128 MB DDRAM		
Memory Protection	CRC		
Program and Data Memory	10 MB less 4 kB for CRCs	5 MB less 64 kB for CRCs	5 MB less 64 kB for CRCs
No. of User Programs	Maximum: 32		
No. of Event Definitions	Maximum: 20000		
Non-volatile Event Buffer	5000 events		
Date/Time Buffer	Min. 5 days, gold capacitor		
Parameter: Communication Interface: Ethernet			
Connector	4 x RJ-45	2 x RJ-45	4 x RJ-45
Speed	10BASE-T, 100BASE-Tx, 1000BASE-T.	10BASE-T, 100BASE-Tx.	10BASE-T, 100BASE-Tx.
Auto-negotiation/crossover	Yes		
Parameter: Communication Interface: Fieldbus			
Connector	X-COM		9-pole D-sub
Protocols	Safeethernet, OPC, SNTP, PROFIsafe, PROFINET, ComUserTask, Modbus.		
Connections	Total: 255, Redundant: 255, Between two controllers: 64.		
Parameter: Environmental Specifications			
Protection IEC/EN 61131-2	Protection class III, IP20		
Operating Temperature	0...+60°C		
Storage Temperature	-40...+85°C		
Maximum Relative Humidity	95%		
Pollution IEC/EN 60664-1	Pollution degree II		
Altitude	<2000 m		

Table B2: HIMax DI and DO Module Datasheet.

DI Module Parameter	X-DI 16 01 [134]	X-DI 32 01 [135]	X-DI 64 01 [136]
Channels	16	32	64
Input Type	Current sinking logic		
Module Cycle Time	Cycle time of the user program		
Rated Input Voltage	0...48/120 VAC	0...24 V	
Input Voltage	0...130 VAC	-3...30 V	
Maximum Input Current	5 mA	2.5 mA	2.9 A
Switching Point	31.6 VAC	9.3 V±10.4 V	
Low Voltage Detection at	25 VAC	16 V	17 V
DO Module Parameter	X-DI 2 02 [137]	X-DI 24 02 [138]	X-DI 32 01 [139]
Channels	12	24	32
Galvanic Isolation	Available		
External supply voltage	24 VDC, -15...+20%		
Output Voltage	Supply voltage minus internal voltage drop		
Voltage Drop	1.3 V at 2 A output current		
Nominal Rated Current	2 A	0.5 A	
Total Current	Maximum: 12 A		
Leakage Current	Maximum: 500 μA		
Overcurrent Interruption	2.5 A	0.75 A	0.8 A
S/C Limiting Current	6 A	2 A	
Ohmic Load	2 A	0.5 A	
Maximum Inductive Load	10 H	1 H	10 H
Maximum Capacitive Load	100 μF		
Overload Protection	33 V	60 V	33 V
Channel Switching Time	200 μs	100 μs	
Test Pulse	200 μs		

Environmental Specifications	
Protection IEC/EN 61131-2	Protection class III, IP20
Operating Temperature	0...+60°C
Storage Temperature	-40...+85°C
Maximum Relative Humidity	95%
Pollution IEC/EN 60664-1	Pollution degree II
Altitude	<2000 m

Table B3: HIMax Counter Module Datasheet.

Parameter	X-CI 24 01 [140]
Channels	24
Channel Pairs	12
Supply Voltage	24 VDC, -15%...+20%
Sensors	Proximity switches
Count frequency	0...10 kHz for proximity switches, 0...20 kHz for control circuit devices
Resolution	0.1 Hz
Counter Resolution	32-bit
Minimum Pulse Width	033.33 μs at 10 kHz 16.66 μs at 20 kHz
Accuracy of Pulse Count	$\pm$1 pulse
Safety-related Accuracy	$\pm$1 % of final value
Protection IEC/EN 61131-2	Protection class III, IP20
Operating Temperature	0...+60 °C
Storage Temperature	-40...+85 °C
Maximum Relative Humidity	95%
Pollution IEC/EN 60664-1	Pollution degree II
Altitude	<2000 m

B.2 ControlSafe Platform (CSP)

Table B4: CSP Datasheet.

Parameter: Processor Details [54], [141], [142]	
Type	NXP QorIQ P2020, NXP QorIQ P1011.
Architecture	e500
Instruction Set	32-bit
No. of Cores/Processor	2 (P2020), 1 (P1011).
No. of Threads/Core	1 (P2020), 1 (P1011).
Core Frequency	800-1300 MHz (P2020), 533-800 MHz (P1011).
Parameter: Memory Details [54], [141], [142]	
L1 Data Cache	32 KB
L1 Instruction Cache	32 KB
L2 Cache/Core	512 KB (P2020), 256 KB (P1011).
L2 Cache ECC Support	Available
L2 Cache Configurability	As SRAM and stashing memory
Maximum Memory Size	1 GB/4 GB (P2020), 512 MB/2 GB (P1011).
Memory Type	DDR3-800 SDRAM (P2020), DDR3-667 SDRAM (P1011).

Table B4 Contd.	
NOR Flash Memory	2x128 MB (P2020), 2x64 MB (P1011).
MRAM	2x2 MB (P2020), 1x2 MB (P1011).
Parameter: Redundancy [54], [55]	
Voting Mechanism	Dual Redundant 2oo2
Lockstep Mechanism	Data Lockstep
Synchronization	SRB and DCA.
Parameter: Expansion Option [141], [142]	
No. of GbE Ports	3 (P2020), 3 (P1011).
No. of PCI Express Lanes	3 (P2020), 2 (P1011).
Serial RapidIO	2 (P2020)
USB 2.0	2 (P2020), 2 (P1011)
Memory Card	SD/MMC
Other Interfaces	SPI, 2xI2C, DUART.
Parameter: Fault Management [54]	
	Hardware-based: checks for latencies, Software-based: checks diagnostics.
Parameter: DI Module [56]	
Channels	8
Input Voltage	24 VDC
Parameter: DO Module [56]	
Channels	8
Output Voltage	24 VDC
Power Consumption	8W
Parameter: Counter Module [56]	
Channels	4
Limit	Up to 10KHz
Parameter: Remote I/O [60]	
Description	Expansion Box Platform
Parameter: Railway Interfaces [54]	
Description	MVB, CAN, UART
Parameter: Communication [54], [59]	
Ports	2 x RJ-45, 10/100/1000 BASE-T
Isolation Voltage	500 VAC
Topology	Ring
Other Interfaces	WLAN, GPS
Parameter: Power Supply [54]	
Input Voltage	90-264VAC
Parameter: Safety Certification [62]	
Compliant Standards	EN50126: 1999 (SIL4), EN 50128: 2011 (SIL4), EN50129: 2003 (SIL4), IEC61508: 2010 (SIL3).

Table B4 Contd.	
Parameter: Life-cycle [54]	
Planned Product Life	15 years
Support/Service	25 years
Hardware Availability	99.9999%
Parameter: Environmental Specifications [54]	
Operating Temperature	-40 °C to +60 °C (open), -40 °C to +70 °C (closed).
Cooling	Forced air, Convection cooling
Vibration EN 61373	Category 1, Class B (EN 50155 12.2.11)
Shock EN 61373	Category 1, Class B (IEC 60068-2-27)
Chassis Sealing	Standard: IP20, Optional: IP30.
Conformal Coating EN 50155	ST1 rating (Salt Mist Test)
Parameter: Other Standards [54]	
Description	EN50121, EN50124, EN50155, EN55024, EN60529, EN60571.

B.3 MH50C

Table B5: MH50C Datasheet.

Parameter: Processor Details [68], [143], [144]	
Type	Intel Atom E680T
Architecture	Tunnel Creek (Queens Bay Platform)
Instruction Set	32-bit
No. of Cores/Processor	1
No. of Threads/Core	2
Core Frequency	1600 MHz
Parameter: Memory Details [68], [144]	
L1 Data Cache	24 KB
L1 Instruction Cache	32 KB
L2 Cache/Core	512 KB
L2 Cache ECC Support	Not available
L2 Cache Configurability	As SRAM and stashing memory
Maximum Memory Size	2 GB
Memory Type	DDR2 SDRAM
BIOS Flash Memory	2 MB
FRAM	8 KB
Mass Storage	SSD mSATA 8GB
Parameter: Redundancy [71]	
Voting Mechanism	Dual Redundant 2oo2
Lockstep Mechanism	Hard Lockstep
Synchronization	SyncLayer

Table B5 Contd.	
Parameter: Expansion Option [68], [144]	
No. of GbE Ports	4
No. of PCI Express Lanes	4
USB 2.0	6
Memory Card	SD/MMC
Other Interfaces	SPI, 2xI2C, DUART.
Parameter: Fault Management [68]	
	Software-based: checks for voltage, temperature and internal errors of FPGA, CPUs, and clock.
Parameter: DI Module [72]	
Channels	16
Input Voltage	24 V, 48 V, 72 V, 96 V, 110 V nom.
Input Current	1 mA to 10 mA, pulsed.
Supply Voltage	10.8 V to 13.2 V
Power Consumption	Typical: 1.6 W, Maximum: 2.6 W.
Parameter: DO Module [73], [74]	
Channels	8
Output Voltage	24 V, 48 V, 72 V, 96 V, 110 V nom.
Output Current	Channel: 300mA, Total: 1200 mA.
Supply Voltage	10.8 V to 13.2 V
Power Consumption	Typical: 1.6 W, Maximum: 2.5 W.
Parameter: Remote I/O Module [75]	
Description	KT4, KT8.
Parameter: Railway Interfaces [71]	
Description	MVB, CAN, Profinet.
Parameter: Communication [71], [145]	
Ports	4 x M12, 100BASE-T
Isolation Voltage	1500 VAC
Topology	Ring
Safe Communication	FSoE
Other Interfaces	WLAN, GPS.
Parameter: Power Supply [146]	
Input Voltage	24 V, 36 V, 48 V, 72 V, 96 V, 110 VDC.
Input Power	14.4 VDC to 154 VDC
Input Current	35 A
Output Voltage	12.6 VDC, 5 VDC and 3.3 VDC.
Output Current	9.5 A, 24 A and 9.1 A
Parameter: Safety Certification [71]	
Compliant Standards	EN50126: 1999, (SIL4) EN 50128: 2011, (SIL4) EN50129: 2003, (SIL4) IEC61508: 2010 (SIL3).

Table B5 Contd.	
Parameter: Life-cycle [71]	
Planned Product Life	10 years
Support/Service	25 years
Hardware Availability	Unlimited in time
Parameter: Environmental Specifications [67]	
Operating Temperature	-40 °C to +60 °C (open), -40 °C to +85 °C (closed)
Cooling	Forced air, Convection cooling
Vibration/Shock	EN 50155: Rolling stock, vehicle body class B, EN 50125-3: Wayside, at least 3 m off the track
Chassis Sealing	Standard: IP20
Altitude	-300 m to +3000 m
Pollution Degree	PD 2
Parameter: Other Standards [67]	
Description	EN50121, EN50124, EN50155, EN55024, EN60529, EN60571.

B.4 VxWorks 7

Table B6: VxWorks 7 technical specifications.

Parameter: OS Properties [82]	
Architecture	Microkernel
Inter Process Communication	Shared memory
Scheduling Policy	Priority-based pre-emptive, round-robin, adaptive scheduling.
Time and Space Partitioning	Available
Memory Protection	Yes
AMP/SMP/BMP Support	Available
Processor Support	32-bit, 64-bit.
Board Support	Arm, Power Architecture, Intel, RISC-V.
POSIX Compliance	Yes
Virtualization	Available
Backward Compatibility	Available with VxWorks 6.x
Networking	IPv4/IPv6, TSN: PTP IEEE 1588-2008, 802.1AS-rev, 802.1Qbv, 802.1Qbu.
Connectivity	IEEE 1394, Socket CAN, USB (host, target, and OTG), OPC-UA.
File System	dosFS (FAT-compatible), HRFS with configur- able commit NAND and NOR flash support.
Multimedia Support	OpenVG, OpenGL ES1/2, JPEG, PNG, PCM Audio, OpenCV.

Table B6 Contd.	
Security	Secure boot: digitally signed image. Secure ELF loader: digi-signed applications. Secure storage: encrypted disk and container. Kernel hardening: non-executable pages, stack guard pages, optional support for KPTI, code and read-only data protection. User management: security events, built-in access controls, AD/LDAP support. Arm Trustzone (OP-TEE support), TPM 2.0. Network security protocols: SSL, SSH, IPsec, IKE, GDOI, SCEP and Firewall.
Safety Certifications	IEC 61508: 2010 (SIL 3)
Parameter: Toolchain [85]	
Name	Workbench 3.3
Framework	Eclipse 3.6, Eclipse CDT project 7.0
Languages	C11, C++17, Python 3.8, Rust.
Compiler	PowerPC: GCC, ARM and Intel: LLVM, Wind River DIAB Compiler.
Debugger	Target debugging agent for VxWorks
Simulator	VxWorks Simulator
Configuration Tools	VxWorks Kernel Configurator
Run-Time Analysis Tools	System Viewer, Performance Profiler, Memory Analyzer, Data Monitor, Code Coverage Analyzer
Additional Tools	Wind River Workbench On-Chip Debugging 3.3, Wind River ICE 2, Wind River Probe, IPL Cantata++ for Wind River Workbench.
Host OS Support	32- and 64-bit:Fedora 13, Novell SUSE Linux, Red Hat Enterprise Linux, Ubuntu, Windows 7 32-bit: Windows XP Professional.
Target OS Support	VxWorks: 5.x, 6.x, 7, Linux, Other OS: via IDE On-Chip Debugging.
Target Architecture	ARM/Xscale, IA-32 and Intel 64, MIPS, PowerPC, Renesas SuperH, ColdFire.
Safety Certifications	IEC 61508: 2010 (SIL 3)
Parameter: BSP Support	
CSP	Available [147]
MH50C	Available [148]

B.5 QNX OS for Safety (QOS)

Table B7: QOS technical specifications.

Parameter: OS Properties [90], [91]	
Architecture	Microkernel
Inter Process Communication	Message passing
Scheduling Policy	Priority-based pre-emptive and other methods.
Time and Space Partitioning	Available (adaptive)
Memory Protection	Yes
AMP/SMP/BMP Support	Available
Processor Support	32-bit, 64-bit
POSIX Compliance	Yes
Virtualization	Available
Backward Compatibility	Available
Networking	IPv4/IPv6
Connectivity	Wifi 802.11 a/b/g/n; USB 3.x, Host, Device, and OTG support; Bluetooth v4.2 Classic and Low Energy protocols and profiles.
File System	DOS, HFS+, Image, RAM, Flash, QNX, Linux, CD-ROM, DVD, NFS, NTFS, CIFS.
Multimedia Support	HTML5, Kanzi, OpenGL ES, Qt 5, Storyboard.
Security	Secure boot: Trust zone /TPM Cryptography: AES 256 Self-verifying file systems, integrity measurement, mandatory access control, rootless execution, address space layout randomization.
Safety Certifications	IEC 61508: 2010 (SIL 3)
Parameter: Toolchain [94]	
Name	QNX Momentics Tool Suite
Framework	Eclipse
Languages	C11, C++14, HTML5, QT, Python, Perl.
Compiler	GCC
Debugger	GDB
Run-Time Analysis Tools	System Profiler, Valgrind Runtime Error Detection, Code Coverage, Target Monitoring.
Host OS Support	Windows, Linux, macOS.
Target OS Support	QNX legacy OS.
Safety Certifications	IEC 61508: 2010 (SIL 3)
Parameter: BSP Support	
CSP	Available [149]
MH50C	Available [150]

B.6 INTEGRITY

Table B8: INTEGRITY technical specifications.

Parameter: OS Properties [96]	
Architecture	Microkernel
Scheduling Policy	Priority-based pre-emptive
Time and Space Partitioning	Available, Enhanced Partition Scheduler
Memory Protection	Yes
AMP/SMP/BMP Support	Available, No BMP
Processor Support	32-bit, 64-bit.
Board Support	PowerPC, Altera, AMD, ARM, NXP, Fujitsu Marvell, Renesas, MIPS, Intel, TI, Xilinx.
POSIX Compliance	Yes
Virtualization	Available
Backward Compatibility	Available
Networking	IPv4/IPv6
Connectivity	USB 1.1,2.0,3.0, Bluetooth, NFC.
File System	DOS/FAT 12/16/32, ISO9660, Wear Leveling NOR/NAND, Flash File Systems, NFS.
Multimedia Support	PEG, OpenGL.
Security	Secure boot, Secure asset and intellectual property: digital signing service, certificates Secure data: unique device keys Cryptography: TLS/SSL stack, FIPS 140-2 library, SSH stack, IPsec/IKE stack.
Safety Certifications	IEC 61508: 2010 (SIL 3), EN 50128: 2011 (SIL 3/4).
Parameter: Toolchain [99]	
Name	MULTI IDE 7
Framework	Eclipse, Rhapsody, Emacs, vi.
Languages	C, C++, EC++, Ada.
Compiler	Green Hills Optimizing Compilers
Debugger	TimeMachine Debugging Suite
Run-Time Analysis Tools	PathAnalyzer, DoubleCheck, Memory Allocations, Run Time Error Checking, OSA Explorer, Profiler.
Host OS Support	Windows, Linux.
Target OS Support	INTEGRITY, Linux, VxWorks, Windows, OSE, ThreadX.
Target Architecture	ARM, Tricore, Intel, MIPS, PowerPC, Renesas, ColdFire.
Safety Certifications	IEC 61508: 2010 (SIL 3), EN 50128: 2011 (SIL 3/4).

Table B8 Contd.	
Parameter: BSP Support [151]	
CSP	Legacy PowerPC: Available
MH50C	Legacy Intel x86: Available

B.7 PikeOS

Table B9: PikeOS technical specifications.

Parameter: OS Properties [71], [103]	
Architecture	Microkernel
Scheduling Policy	Priority-based pre-emptive
Time and Space Partitioning	Available
Memory Protection	Yes
AMP/SMP/BMP Support	Available, No BMP
Processor Support	32-bit, 64-bit
Board Support	PowerPC, x86, ARM, Renesas, Sparc V8/LEON.
POSIX Compliance	Yes
Virtualization	Available
Backward Compatibility	Available
Networking	IPv4/IPv6
Connectivity	USB
File System	NAND/NOR Flash, MMC Mass Storage.
Multimedia Support	GPU drivers
Security	Communication encryption, binary verification, MILS compliant.
Safety Certifications	IEC 61508: 2010 (SIL 3), EN 50128: 2011 (SIL 4).
Parameter: Toolchain [105]	
Name	CODEO
Framework	Eclipse
Languages	C, C++.
Compiler	GCC
Debugger	Graphical remote debugger
Simulator	Simulation Targets
Run-Time Analysis Tools	static system analysis, remote system explorer, PikeOS monitor, partition control, application and kernel tracing.
Host OS Support	32-and 64-bit: Windows 7, 8, 10, Linux.
Target OS Support	PikeOS, Linux, Android, ARINC 653, AUTOSAR, RTEMS, legacy RTOS.
Target Architecture	ARM, PowerPC, x86, Sparc.
Safety Certifications	IEC 61508 (SIL3), EN 50128 (SIL4).

Table B9 Contd.	
Parameter: BSP Support [152]	
CSP	Legacy PowerPC: Available
MH50C	Legacy Intel x86: Available

B.8 SCADE

Table B10: SCADE technical specifications.

Parameter: IDE Properties [112]	
Framework	SCADE language (Model Based Programming)
Development Tools	SCADE Architect, SCADE LifeCycle, SCADE Test, SCADE Display, Riming and Stack Optimizer, Design Verifier, Configuration Management Tools and Gateway, Python- and JAVA-based API, Library for integrators, hysteresis,quantizers, filters.
Parameter: Code Generation [112]	
Type	C, Ada
Code Portability	VxWorks 653, VxWorks CERT, INTEGRITY-178B, PikeOS, DDC-I Deos, Customizable RTOS Adaptors.
Compiler	KCG
Debugger	Proprietary
Safety Certification	IEC 61508: 2101 (SIL 3), EN 50128: 2011 (SIL 3/4).
Certification Package	Tool Qualification Plan, Tool Operational Requirements, Tool Accomplishment Summary or Safety Case, Compliance Analysis to standards.
Parameter: Host System [112]	
Operating System	Windows
RAM	Minimum: 1 GB, Recommended: 2 GB.
Disk Space	Minimum: 1 GB
Connectivity	TCP/IP

B.9 FlexiSafe

Table B11: FlexiSafe technical specifications.

Parameter: IDE Properties [116]	
Framework	ISaGRAF
Languages	IEC 61131-3, IEC 61499, C.
Development Tools	Cause and Effect Editor, Dependency Tree, Static Checker, Version Source Control, Cross Reference Browser, PLCopen Safety Function Blocks Library.
Parameter: Code Generation [116]	

Table B11 Contd.	
Type	C
Code Portability	Any
Target Hardware	1oo1D, 1oo2D, 2oo2D, 2oo3.
Compiler	Proprietary
Debugger	Proprietary
Safety Certification	IEC 61508: 2010 (SIL 3), EN 50128: 2011 (SIL 4).
Certification Package	Certification evidence of development environment and procedures, test reports on TIC instructions, relevant FlexiSafe and OS Safety manuals.
Parameter: Host System [116]	
Operating System	Windows
RAM	2 GB
Connectivity	Ethernet, USB.

B.10 Prover Trident

Table B12: Prover Trident technical specifications.

Parameter: IDE Properties [121]	
Framework	Formal methods
Development Tools	PiSPEC IP and Prover iLock suite
Parameter: Code Generation [121]	
Type	C and Ada.
Code Portability	Any
Target Hardware	Any
Compiler	Prover iLock Coder
Debugger	Prover iLock Simulator
Safety Certification	EN 50128: 2011 (SIL 4)
Parameter: Host System [121]	
Operating System	Windows

B.11 CODESYS Safety

Table B13: CODESYS Safety technical specifications.

Parameter: IDE Properties [124]	
Framework	CODESYS Development System
Languages	IEC 61131-3
Development Tools	CODESYS UML, Profiler, Test Manager, Static Analysis, SVN, Application Composer, Safety NetVars, PLCopen Safety Function Block Library, Safety Fieldbus.

Table B13 Contd.	
Parameter: Code Generation [124]	
Type	C
Code Portability	Windows and QNX.
Target Hardware	TriCore, ARM, PowerPC.
Compiler	Proprietary
Debugger	Proprietary
Safety Certification	IEC 61508: 2010 (SIL 3)
Certification Package	Safety integration and test manual: integration interfaces with hardware abstract and adoptions; safety verification package: framework for OEM tests; CODESYS Test Manager: generation of automated test cases, instruction and reports; approved safety manual for users.
Parameter: Host System [124]	
Operating System	Windows

C Annexes of Standards

C.1 IEC 61508: 2010

IEC 61508 – 2

Table C1: Annexes of Part 2 of IEC 61508: 2010.

Annex A	Demonstration of techniques for controlling failures during operation for hardware components, such as CPU, I/O, power supply, electromechanical devices, bus, clock, etc.
Annex B	Demonstration of techniques for avoiding systematic failures at different life-cycle phases via project management, documentation, separation between safe and non-safe functions, formal and semi-formal methods, etc.
Annex C	Calculation of diagnostic coverage and safe failure fraction by categorizing failure modes and performing Failure Mode and Effect Analysis (FMEA).
Annex D	Guidance for compiling safety manual containing functional specifications, failures modes, respective failure rates, constraints, etc.
Annex E	Illustration of requirements for Integrated Circuits (IC) with on-chip redundancy focusing on avoiding failures, implementing watchdog and other monitoring elements, separate physical blocks, etc.
Annex F	Requirement specifications for application-specific integrated circuits (ASIC) at the design, synthesis, testing, and manufacturing level.

IEC 61508 – 3

Table C2: Annexes of Part 3 of IEC 61508: 2010.

Annex A	Depiction of different techniques and measures for software development to achieve a particular SIL in terms of, architectural design, support tools and programming language, software module testing and integration,hardware and software integration methods, software validation and verification functional safety assessment, etc.
Annex B	Detailed tables from Annex A concerning design and coding standards, dynamic analysis and testing, functional and black-box testing, failure analysis, modelling, performance testing, etc.
Annex C	Guidance for choosing a set of techniques described in the Annexes.
Annex D	Instructions on preparing a safety manual for software elements.
Annex E	Representation of common software requirements described in IEC 61508-2 and IEC 61508-3.

Table C2 Contd.	
Annex F	Description of isolation between different software elements in a single computer system in terms of spatial/temporal independences.
Annex G	Guidance for life-cycles related with the system and application part of the software for different variability programming and application configurability profiles.

IEC 61508 – 5

Table C3: Annexes of Part 5 of IEC 61508: 2010.

Annex A	Representation of individual and societal risks, different risk profiles, modes of operations, allocation of safety functions, etc.
Annex B	Overview of all the methods described in the following annexes and criteria for adopting a method based on risk acceptance condition, operating mode of safety functions, gravity of consequences, etc.
Annex C	As low as reasonably practicable (ALARP) method where the risk is reduced at a level to achieve a particular SIL.
Annex D	A quantitative method used for quantifiable risks.
Annex E	Risk graph methods, a qualitative method where SIL is calculated from risk factors associated with the EUC.
Annex F	Layer of protection analysis (LOPA).
Annex G	Hazardous event severity matrix, a qualitative method used for unquantifiable risks.

IEC 61508 – 6

Table C4: Annexes of Part 6 of IEC 61508: 2010.

Annex A	Overview of applications of IEC 61508-2 and IEC 61508-3.
Annex B	Evaluation of probabilities of hardware failure via static and dynamic models, and Monte Carlo simulation techniques with examples.
Annex C	Example calculation of diagnostic coverage and safe failure fraction.
Annex D	Quantification of the effect of hardware-related common cause failures by using the β-factor and shock models.
Annex E	Description of software requirements for two use cases requiring SIL 2 and SIL 3 in terms of, safety requirements, architectural design, support tools and programming languages, testing and integration, verification, validation, and functional safety assessment.

IEC 61508 – 7

Table C5: Annexes of Part 7 of IEC 61508: 2010.

Annex A	Control of random hardware failures concerning electromechanical and electronic components, CPUs, variable and invariable memory ranges, I/O, communication interfaces, mass-storage, power supply, ventilation, environmental conditions, sensors, actuators, etc.
Annex B	Avoidance of systematic failures via project management, proper documentation, isolating safety functions from non-safety functions, usage of formal methods, finite state machines, time petri nets, etc. and different testing methods, such as functional testing, black-box testing, statistical testing etc., safety validation through static and dynamic analyses, and failure analysis techniques.
Annex C	Achieving required software safety integrity by using structural diagrammatic methods, such as Controlled Requirements Expression (CORE), Jackson System Development (JSD), real-time Yourdon etc.; implementing architectural design measures, e.g. fault detection and diagnosis, error detecting/correcting codes, diverse programming, applying proper development tools and languages, certified compilers, verification methods, e.g. control and data flow analyses, etc.
Annex D	Determining software safety integrity in pre-developed software, auch as operating systems, libraries, compilers, etc. by statistical methods for low and high demands of operation.
Annex E	Designing ASICs in very high speed integrated circuit hardware description language (VHDL) or Verilog by following guidelines for schematic entry, structured description, using tools, simulation, functional testing, coding style, etc.
Annex F	Definition of properties at different software life-cycle phases.
Annex G	Guidance for safety-related object oriented software development.

C.2 EN 50126: 2017

EN 50126 – 1

Table C6: Annexes of Part 1 of EN 50126: 2017.

Annex A	Guidance and an example illustrating methods and tools for developing and managing a basic RAMS plan.
Annex B	Display of different reliability, availability, maintenance and safety parameters for a railway system.
Annex C	Illustration on developing a risk matrix.
Annex D	Description of functional definitions of a system.

EN 50126 – 2

Table C7: Annexes of Part 2 of EN 50126: 2017.

Annex A	Description of methods, e.g. ALARP, Globalement Au Moins Equivalent (GAME) and minimum endogenous mortality (MEM) to define risk acceptance criteria.
Annex B	Demonstration of calculating total hazard rate (THR) from accident and failure statistics.
Annex C	Guidance on SIL allocation.
Annex D	Illustration of qualitative and quantitative apportionment of system to assign SIL.
Annex E	Description of probabilistic mistakes which generates errors.
Annex F	Description of different techniques, such as HAZOP, FMEA, ETA, FMECA, FTA, RBD, etc. for safety analysis.
Annex G	Definition of the roles and responsibilities of requirements manager, designer, implementer, tester, verifier, integrator, validator, assessor, project manager, and configuration manager.

C.3 EN 50128: 2011

Table C8: Annexes of EN 50128: 2011.

Annex A	Selection of techniques and measures to achieve required SIL for an application, e.g. life-cycle issues, documentation, software requirements specification, software architecture, software design and implementation, verification and testing, integration, overall software testing, software analysis techniques, software quality assurance, software maintenance, data preparation, coding standards, dynamic analysis and testing, textual and diagrammatic programming languages, modelling, performance testing, static analysis, code coverage, object oriented software architecture and design, etc.
Annex B	Definition of the roles and responsibilities of requirements manager designer, implementer, tester, verifier, integrator, validator, assessor, project manager, and configuration manager.
Annex C	Illustration of which of the previously mentioned actors in Annex B will write and check all the documents.
Annex D	Bibliography of all the techniques mentioned in Annex A.

Software Design and Implementation

Table C9: Annexes of EN 50128: 2011.

Techniques	SIL 0	SIL 1	SIL 2	SIL 3	SIL 4
Formal Methods	-	R	R	HR	HR
Modelling	R	HR	HR	HR	HR
Structured Methodology	R	HR	HR	HR	HR
Modular Approach	HR	M	M	M	M
Components	HR	HR	HR	HR	HR
Design and Coding Standards	HR	HR	HR	M	M
Analysable Programs	HR	HR	HR	HR	HR
Strongly Typed Programming Language	R	HR	HR	HR	HR
Structured Programming	R	HR	HR	HR	HR
Programming Language	R	HR	HR	HR	HR
Language Subset	-	-	-	HR	HR
Object Oriented Programming	R	R	R	R	R
Procedural Programming	R	HR	HR	HR	HR
Metaprogramming	R	R	R	R	R

Programming Languages

Table C10: Annexes of EN 50128: 2011.

Languages	SIL 0	SIL 1	SIL 2	SIL 3	SIL 4
ADA	R	HR	HR	HR	HR
MODULA-2	R	HR	HR	HR	HR
PASCAL	R	HR	HR	HR	HR
C/C++	R	R	R	R	R
PL/M	R	R	R	NR	NR
BASIC	R	NR	NR	NR	NR
Assembler	R	R	R	R	R
C#	R	R	R	R	R
JAVA	R	R	R	R	R
Statement List	R	R	R	R	R
Functional Block Diagrams	R	R	R	R	R
Sequential Function Charts	-	HR	HR	HR	HR
Ladder Diagram	R	R	R	R	R
State Charts	R	HR	HR	HR	HR

The requirements are categorized as per the following:

'-': no recommendation for or against being used.

'NR': Not Recommended for the particular safety integrity level.

'R': Recommended for the particular safety integrity level.

'HR': Highly Recommended for the particular safety integrity level.

'M': Mandatory for the particular safety integrity level.

C.4 EN 50129: 2018

Table C11: Annexes of EN 50129: 2018.

Annex B	Overview, detection, and effects of random hardware faults and systematic faults, and methods applied against them.
Annex C	Overview of failure modes of different hardware components, such as resistors, capacitors, electromagnetic components, diodes, transistors, controlled rectifiers, surge suppressors, optoelectronic components, filters, switches, buttons, fuses, lamps, batteries, etc.
Annex D	Illustration of an example about how to define THR, TFFR and FR for a safety-critical process and allocate SIL.
Annex E	Overview of techniques and measures adopted to control and avoid systematic and random faults.
Annex F	Guidance on using user-programmable integrated circuits (UPICs) within a safety architecture.
Annex G	Overview of changes from the previous version, EN 50129:2003.

C.5 EN 50159: 2010

Table C12: Annexes of EN 50129: 2018.

Annex A	Overview on sources and consequences of threats, such as repetition, deletion, insertion, delay, corruption, message masquerading, etc., and outline for compiling a safety case based on hazard analysis.
Annex B	Overview of characteristics of different types of transmission systems and the threats associated with them.
Annex C	Discussions on possible threat-aversion mechanisms, such as use of time stamps, safety codes, e.g. main, linear, cyclic, hash and cryptographic block codes, use of digital signatures, etc.
Annex D	Use cases on using the standard.
Annex E	Mapping of parts with the previous version, EN 50159: 2001.